BROADBAND GATE

インターネットVPN対応ブロードバンドルータ

FutureNet XR-410/TX2シリーズ

ユーザーズガイド

Ver1.4.1対応版

センチュリー・システムズ 株式会社

目次

はじめに 6
ご使用にあたって 7
パッケージの内容物の確認 10
第1章 XR-410の概要 11
I. XR-410/TX2シリーズの特長 12
II. 各部の名称と機能 14
III. 動作環境 15
第2章 XR-410の設置 16
XR-410の設置 17
第3章 コンピューターのネットワーク設定 18
I. Windows 95/98/Meのネットワーク設定 19
II. Windows 2000のネットワーク設定 20
III. Windows XPのネットワーク設定 21
IV. Macintoshのネットワーク設定 22
V. IPアドレスの確認と再取得 23
第4章 設定画面へのログイン 24
設定画面へのログイン方法 25
第5章 インターフェース設定 26
I.Ethernetポートの設定 27
II.Ethernetポートの設定について 29
III.Ethernetブリッジの設定 30
IV.通常接続(CATVなど)での接続設定例 31
V.ローカルルータ設定 32
第6章 PPPoE設定 33
I. PPPoEの接続先設定 34
II. PPPoEの接続設定と回線の接続/切断 36
III.その他の接続設定 37
IV.副回線とバックアップ回線 38
V.PPPoE特殊オプション設定について 41
第7章 RS-232ポートを使った接続(リモートアクセス機能) 42
I. XR-410とアナログモデム/TAの接続 43
◆アナログモデム/TAの接続 43
II. リモートアクセス回線の接続先設定 44
III. リモートアクセス回線の接続と切断 46
IV. 副回線接続とバックアップ回線接続 47
第8章 複数アカウント同時接続設定 48
複数アカウント同時接続の設定 49
第9章 各種サービスの設定 53
各種サービス設定 54
第10章 DNSリレー/キャッシュ機能 55
I. DNSキャッシュ機能の概要 56
II. DNSキャッシュ機能の設定 57
第11章 DHCPサーバ/リレー機能 58
I. XR-410のDHCP関連機能について 59
II. DHCPサーバ機能の設定 60
III. DHCPサーバ機能の設定例 61
IV. IPアドレス固定割り当て設定 62

第 12 章 IPsec 機能 63
I.XR-410 の IPsec 機能について 64
II.IPsec 設定の流れ 65
III.IPsec 設定 66
IV.IPsec Keep-Alive 機能 73
V.「X.509 デジタル証明書」を用いた電子認証 74
VI.IPsec 通信時のパケットフィルタ設定 76
VII.IPsec がつながらないとき 77
第 13 章 UPnP 機能 80
I.UPnP 機能の設定 81
◆UPnP 機能の設定 81
◆UPnP の接続状態の確認 82
II.UPnP とパケットフィルタ設定 83
◆UPnP 機能使用時の注意 83
◆UPnP 機能使用時の推奨フィルタ設定 83
第 14 章 ダイナミックルーティング(RIP と OSPF の設定) 84
I. ダイナミックルーティング機能 85
◆設定の開始 85
II. RIP の設定 86
◆RIP の設定 86
◆RIP フィルターの設定 87
III. OSPF の設定 88
◆インタフェースへの OSPF エリア設定 88
◆OSPF エリア設定 89
◆OSPF VirtualLink 設定 90
◆OSPF 機能設定 91
◆インタフェース設定 93
◆ステータス表示 94
第 15 章 SYSLOG 機能 95
syslog 機能の設定 96
第 16 章 帯域制御(QoS)機能 98
I.QoS 機能の概要 99
II. QoS 機能の設定 100
第 17 章 攻撃検出機能 101
攻撃検出機能の設定 102
第 18 章 SNMP エージェント機能 103
SNMP エージェント機能の設定 104
第 19 章 NTP サービス 105
NTP サービスの設定方法 106
第 20 章 VRRP 機能 107
I.VRRP の設定方法 108
II.VRRP の設定例 109
第 21 章 アクセスサーバ機能 110
I. アクセスサーバ機能について 111
II. XR-410 とアナログモデム /TA の接続 112
◆アナログモデム /TA の接続 112
III. アクセスサーバ機能の設定 113

第 22 章 スタティックルーティング 114
スタティックルーティング設定 115
第 23 章 ソースルーティング 117
ソースルーティング設定 118
第 24 章 NAT 機能 119
I. XR-410 の NAT 機能について 120
II. バーチャルサーバ設定 121
III. 送信元 NAT 設定 122
IV. バーチャルサーバの設定例 123
◆ WWW サーバを公開する際の NAT 設定例 123
◆ FTP サーバを公開する際の NAT 設定例 123
◆ PPTP サーバを公開する際の NAT 設定例 124
◆ DNS、メール、WWW、FTP サーバを公開する際の NAT 設定例(複数グローバルアドレスを利用) 125
V. 送信元 NAT の設定例 126
補足：ポート番号について 127
第 25 章 パケットフィルタリング機能 128
I. 機能の概要 129
II. XR-410 のフィルタリング機能について 130
III. パケットフィルタリングの設定 131
IV. パケットフィルタリングの設定例 133
◆インターネットから LAN へのアクセスを破棄する設定 133
◆ WWW サーバを公開する際のフィルタ設定例 134
◆ FTP サーバを公開する際のフィルタ設定例 134
◆ WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例 135
◆ NetBIOS パケットが外部へ出るのを防止するフィルタ設定 136
◆ WAN からのブロードキャストパケットを破棄するフィルタ設定(smurf 攻撃の防御) 136
◆ WAN からのパケットを破棄するフィルタ設定(IP spoofing 攻撃の防御) 137
◆外部からの攻撃を防止する総合的なフィルタリング設定 137
◆ PPTP を通すためのフィルタ設定 138
V. 外部から設定画面にアクセスさせる設定 139
補足：NAT とフィルタの処理順序について 140
補足：ポート番号について 141
補足：フィルタのログ出力内容について 142
第 26 章 仮想インターフェース機能 143
仮想インターフェースの設定 144
第 27 章 GRE 機能 145
GRE の設定 146
第 28 章 ゲートウェイ認証機能 147
ゲートウェイ認証機能の設定 148
◆基本設定 148
◆ユーザー設定 149
◆ RADIUS 設定 150
◆フィルタ設定 151
◆ログ設定 151
ゲートウェイ認証下のアクセス方法 152
◆ホストからのアクセス方法 152
◆設定画面へのアクセスについて 152
◆ RADIUS 設定について 152

◆認証について 152
ゲートウェイ認証の制御方法について 153
第 29 章 ネットワークテスト 154
ネットワークテスト 155
第 30 章 各種システム設定 158
◆時計の設定 159
◆ログの表示 160
◆ログの削除 160
◆パスワードの設定 161
◆ファームウェアのアップデート 161
◆設定の保存と復帰 162
◆設定のリセット 163
◆本体再起動 164
◆セッションライフタイムの設定 164
◆設定画面の設定 165
第 31 章 情報表示 166
本体情報の表示 167
第 32 章 運用管理設定 168
一時的に工場出荷設定に戻す方法 169
携帯電話による制御 170
携帯電話による操作方法 171
付録 A 工場出荷設定一覧 172
付録 B 製品仕様 174
付録 C サポートについて 177
サポートについて 178

はじめに

◆ご注意

1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承下さい。

2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承下さい。

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡下さい。

◆商標の表示

□「BROADBAND GATE」はセンチュリー・システムズ株式会社の登録商標です。

□「XR-410」はセンチュリー・システムズ株式会社の商標です。

□下記製品名等は米国 Microsoft Corporation の登録商標です。

Microsoft、Windows、Windows 95、Windows 98、Windows NT4.0

Windows 2000、Windows XP

□ Macintosh は、アップルコンピュータ社の登録商標です。

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

本製品を安全にお使いいただくために、まず以下の注意事項を必ずお読み下さい。

絵表示について	この取扱説明書では、製品を安全に正しくお使いいただき、あなたや他の人々への危害や財産への損害を未然に防止するために、いろいろな絵表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

次の表示の区分は、表示内容を守らず、誤った使用をした場合に生じる「危害や損害の程度」を説明しています。

⚠ 危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う危険が差し迫って生じることが想定される内容を示しています。
⚠ 警告	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

次の絵表示の区分は、お守りいただく内容を説明しています。

	このような絵表示は、してはいけない「禁止」を意味するものです。それぞれに具体的な禁止内容が書かれています。
	このような絵表示は、必ず実行していただく「強制」を指示するものです。それぞれに具体的な指示内容が書かれています。

⚠ 危険

必ず本体に付属している電源ケーブルをご使用ください。

使用温度範囲は 0℃～ 40℃です。この温度範囲以外では使用しないでください。

ストーブのそばなど高温の場所で使用したり、放置しないでください。

火の中に投入したり、加熱したりしないでください。

製品の隙間から針金などの異物を挿入しないでください。

ご使用にあたって

⚠ 警告

万一、異物(金属片・水・液体)が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡下さい。そのまま使用すると火災の原因となります。

万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡下さい。

本体を分解、改造しないでください。けがや感電などの事故の原因となります。

本体または電源ケーブルを直射日光の当たる場所や 、調理場や風呂場など湿気の多い場所では絶対に使用しないでください。火災・感電・故障の原因となります。

電源ケーブルの電源プラグについたほこりはふき取ってください。火災の原因になります。

濡れた手で電源ケーブル、コンセントに触れないでください。感電の原因となります。

電源ケーブルのプラグにドライバなどの金属が触れないようにしてください。火災・感電・故障の原因となります。

AC100V の家庭用電源以外では絶対に使用しないでください。火災・感電・故障の原因となります。

ご使用にあたって

⚠ 注意

湿気やほこりの多いところ、または高温となるところには保管しないでください。故障の原因となります。

乳幼児の手の届かないところに保管してください。けがなどの原因となります。

長期間使用しないときには、電源ケーブルをコンセントおよび本体から外してください。

電源ケーブルの上に重いものを乗せたり、ケーブルを改造したりしないで下さい。また、電源ケーブルを無理に曲げたりしないでください。火災・感電・故障の原因となることがあります。

電源ケーブルは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。

近くに雷が発生したときには、AC アダプタをコンセントから抜いて、ご使用をお控え下さい。落雷が火災・感電・故障の原因となることがあります。

AC アダプタのプラグを本体に差し込んだ後に AC アダプタのケーブルを左右および上下に引っ張ったり、ねじったり、曲げたりしないでください。緩みがある状態にしてください。

本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。

高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。万が一不足がありましたら、お買いあげいただいた店舗または弊社サポートデスクまでご連絡ください。

XR-410/TX2またはXR-410/TX2DES本体	1台
リリースノート	1部
製品マニュアル PDF形式(CD-ROM)	1枚
RJ-45/D-sub9ピン変換アダプタ(ストレート)	1個
UTPケーブル(ストレート)	1本
ACアダプタ	1個
保証書	1部

第1章

XR-410の概要

Ⅰ．XR-410/TX2 シリーズの特長

◆高速ネットワーク環境に余裕で対応

XR-410/TX2 シリーズ(以下 XR-410)の Ethernet インターフェースは全て 10base-T/100Base-TX となっており、高速 ADSL や FTTH 等の高速インターネット接続や LAN 環境の構成に充分な性能と機能を備えています。

◆ PPPoE クライアント機能

XR-410 は PPPoE クライアント機能を搭載していますので、FTTH サービスや NTT 東日本 / 西日本などが提供するフレッツ ADSL・B フレッツサービスに対応しています。また、PPPoE の自動接続機能やリンク監視機能、IP アドレス変更通知機能を搭載しています。

◆ unnumbered 接続対応

unnumbered 接続に対応していますので、ISP 各社で提供されている固定 IP サービスでの運用が可能です。

◆ IPsec 通信

IPsec を使うと、通信相手の認証と通信の暗号化により簡単に VPN(Virtual Private Network)を実現できます。WAN 上の IPsec サーバと 1 対 n で通信が可能です。最大対地数は 64 です。
また、公開鍵の作成から IPsec 用の設定、通信の開始 / 停止まで、ブラウザ上で簡単におこなうことができます。

◆ GRE トンネリング機能

仮想的なポイントツーポイントリンクを張って各種プロトコルのパケットを IP トンネルにカプセル化する GRE トンネリングに対応しています。

◆シリアルポートを搭載

XR-410 は RS-232 ポートを備えています。常時接続のルータとして使いながら、同時にモデムや TA を接続してアクセスサーバや、リモートルータとして利用することができます。また、電話回線経由で XR-410 を遠隔管理することも可能です。

◆障害時のバックアップ回線接続機能

VRRP による機器冗長機能だけでなく、OSPF や Ping によるインターネット VPN のエンド～エンドの監視を実現し、ネットワークの障害時に ISDN 回線やブロードバンド回線を用いてバックアップする機能を搭載しています。

◆ステートフルパケットインスペクション機能

動的パケットフィルタリングともいえる、ステートフルパケットインスペクション機能を搭載しています。これは、WAN 向きのパケットに対応する LAN 向きのパケットのみを通過させるフィルタリング機能です。これ以外の要求ではパケットを通しませんので、ポートを固定的に開放してしまう静的パケットフィルタリングに比べて高い安全性を保てます。

◆ゲートウェイ認証機能

XR-410 をインターネットゲートウェイとして運用するときに、インターネットへアクセスするための認証を行う機能を搭載しています。パスワード認証によって外部への不正なアクセスを制限することができます。

Ⅰ．XR-410/TX2 シリーズの特長

◆静的パケットフィルタリング機能
送信元 / あて先の IP アドレス・ポート、プロトコルによって詳細なパケットフィルタの設定が可能です。入力 / 転送 / 出力それぞれに対して最大 256 ずつのフィルタリングポリシーを設定できます。ステートフルパケットインスペクション機能と合わせて設定することで、より高度なパケットフィルタリングを実現することができます。

◆ DHCP クライアント / サーバ機能
DHCP クライアント機能によって、IP アドレスの自動割り当てをおこなう CATV インターネット接続サービスでも利用できます。また、LAN 側ポートでは DHCP サーバ機能を搭載しており、LAN 側の PC に自動的に IP アドレス等の TCP/IP 設定を行なえます。

◆ NAT/IP マスカレード機能
IP マスカレード機能を搭載していることにより、グローバルアドレスが 1 つだけしか利用できない場合でも、複数のコンピューターから同時にインターネットに接続できます。
また静的 NAT 設定によるバーチャルサーバ機能を使えば、プライベート LAN 上のサーバをインターネットに公開することができます。
さらに XR-410 では複数のグローバルアドレスを NAT で設定できます。

◆ローカルルータ / ブリッジ機能
NAT 機能を使わずに、単純なローカルルータ / ブリッジとして使うこともできます。

◆ルーティング機能
スタティックルート設定と RIP はもちろん、OSPF を用いたダイナミックルーティングが可能です。

◆ QoS 機能
IP アドレスとポートによる、帯域制御をおこなうことができます。これにより、ストリーミングデータを利用する通信などに帯域を割り当てることが可能になります。

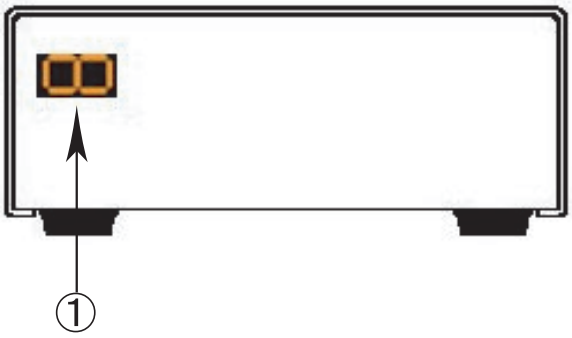
◆ログ機能
XR-410 のログを取得する事ができ、ブラウザ上でログを確認することが可能です。ログを電子メールで送信することも可能です。また攻撃検出設定を行なえば、インターネットからの不正アクセスのログも併せてログに記録されます。

◆バックアップ機能
本体の設定内容を一括してファイルにバックアップすることが可能です。
また設定の復元も、ブラウザ上から簡単にできます。

◆ファームウェアアップデート
ブラウザ設定画面上から簡単にファームウェアのアップデートが可能です。特別なユーティリティを使わないので、どの OS をお使いの場合でもアップデートが可能です。

II．各部の名称と機能

◆製品前面



①7 セグメント LED
本装置の状態を表します。

本装置の起動中は 2 → 3 → 4 → 5 → 6 → 7 の順に LED が表示されます。

本装置の起動後は、本装置の各インタフェースのリンク状態を表示します。以下に各状態について説明します。

Ether0 ポートが Linkup している状態。

Ether1 ポートが Linkup している状態。

RS-232 ポートが Linkup している状態。

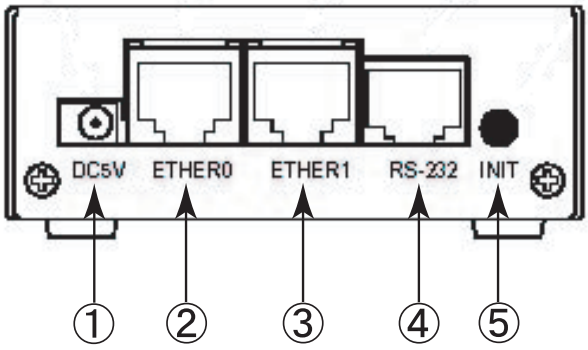
システムが動作している状態。右上にある「。」が点滅します。

ケーブルを接続して動作している状態の表示例。

ファームウェアのアップデート中は「8」が表示されます。

「2」「6」「8」等の数字を表示したまま止まっているときは、システム故障により本装置が正常にが起動できない状態となっています。弊社にてシステムの復旧が必要となりますので、この状態になったときは弊社までご連絡下さい。

◆製品背面



①電源コネクタ
製品付属の AC アダプタを接続します。

② Ether0 ポート
主に LAN との接続に使用します。イーサネット規格の UTP 100Base-TX ケーブルを接続します。ケーブルの極性は自動判別します。

③ Ether1 ポート
WAN 側ポートとして、また、Ether0 ポートとは別セグメントを接続するポートとして使います。イーサネット規格の UTP 100Base-TX ケーブルを接続します。ケーブルの極性は自動判別します。

④ RS-232 ポート
リモートアクセスやアクセスサーバー機能を使用するときにモデムを接続します。ストレートタイプの LAN ケーブルと製品添付の変換アダプタを用いてモデムと接続してください。

⑤ INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに押します。操作方法については第 32 章をごらんください。

III. 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

- 本製品に接続するコンピューターの全てに、10Base-T または 100Base-TX の LAN ボード / カードがインストールされていること。
- ADSL モデムまたは CATV モデムに、10Base-T または 100Base-TX のインターフェースが搭載されていること。
- 本製品と全てのコンピューターを接続するためのハブやスイッチングハブが用意されていること。
- 本製品と全てのコンピューターを接続するために必要な種類のネットワークケーブルが用意されていること。
- シリアルポートを使う場合は、接続に必要なシリアルケーブルが用意されていること。

◆ソフトウェア環境

- TCP/IP を利用できる OS がインストールされていること。
- 接続されている全てのコンピューターの中で少なくとも 1 台に、InternetExplorer4.0 以降か NetscapeNavigator4.0 以降がインストールされていること。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承下さい。

第2章

XR-410の設置

XR-410 の設置

XR-410 と xDSL/ ケーブルモデムやコンピューターは、以下の手順で接続してください。

1 本装置と xDSL/ ケーブルモデムやパソコン・HUB など、接続する全ての機器の電源が OFF になっていることを確認してください。

2 本装置の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。

3 本装置の背面にある Ether0 ポートと HUB や PC を、LAN ケーブルで接続してください。

各 Ethernet ポートは LAN ケーブルの極性を自動判別します。

4 本装置と AC アダプタ、AC アダプタとコンセントを接続して下さい。

5 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

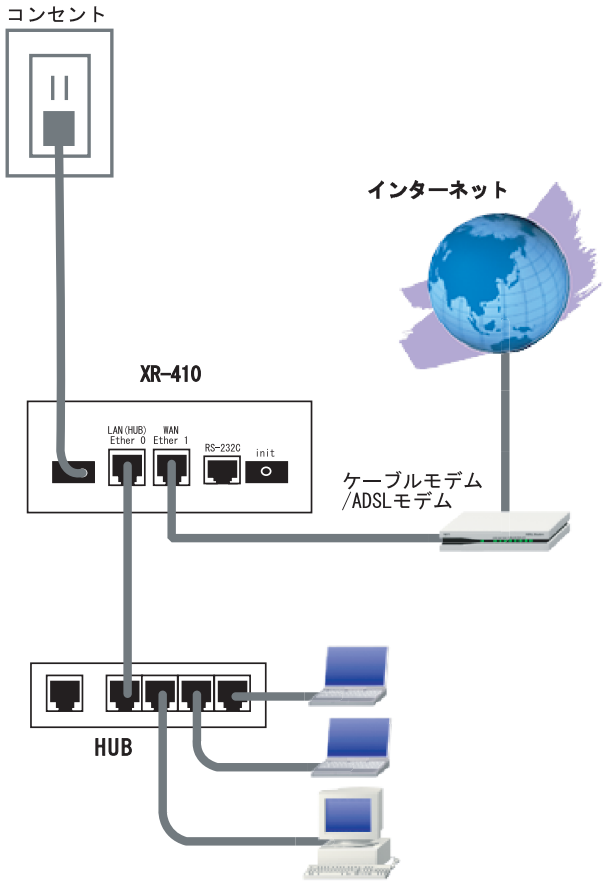
⚠ 注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。内部温度が上がり、動作が不安定になる場合があります。

⚠ 注意！

AC アダプターのプラグを本体に差し込んだ後に AC アダプターのケーブルを左右及び上下に引っ張らず、緩みがある状態にして下さい。
抜き差しもケーブルを引っ張らず、コネクタを持っておこなってください。
また、AC アダプターのケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

接続図(例)



⚠ 注意！

XR-410 側でも各ポートで ARP table を管理しているため、PC を接続しているポートを変更するとその PC から通信ができなくなる場合があります。このような場合は、XR-410 側の ARP table が更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

第3章

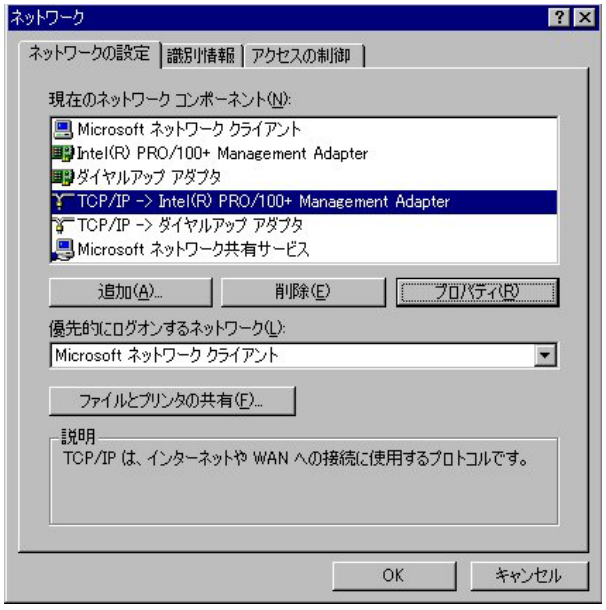
コンピューターのネットワーク設定

第3章 コンピューターのネットワーク設定

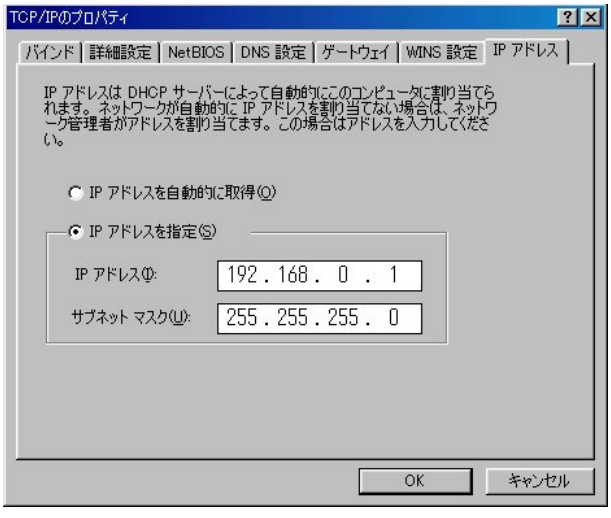
I. Windows 95/98/Me のネットワーク設定

ここでは Windows95/98/Me が搭載されたコンピューターのネットワーク設定について説明します。

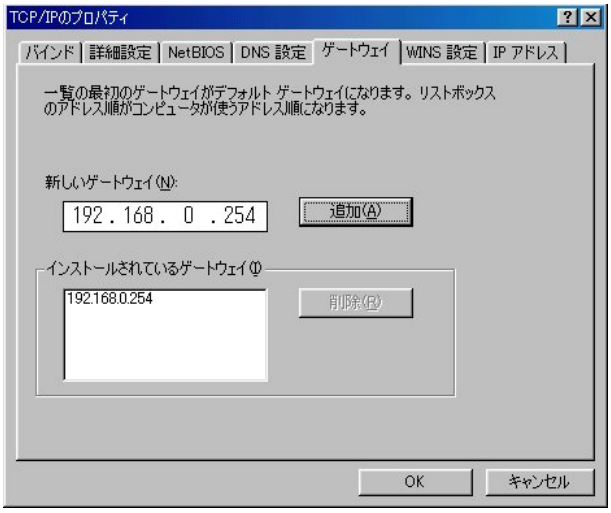
1 「コントロールパネル」→「ネットワーク」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピューターに装着された LAN ボード(カード)のプロパティを開きます。



2 「TCP/IP のプロパティ」が開いたら、「IP アドレス」タブをクリックして IP 設定をおこないます。「IP アドレスを指定」にチェックを入れて、IP アドレスに「192.168.0.1」、サブネットマスクに「255.255.255.0」と入力します。



3 続いて「ゲートウェイ」タブをクリックして、新しいゲートウェイに「192.168.0.254」と入力して追加ボタンをクリックしてください。



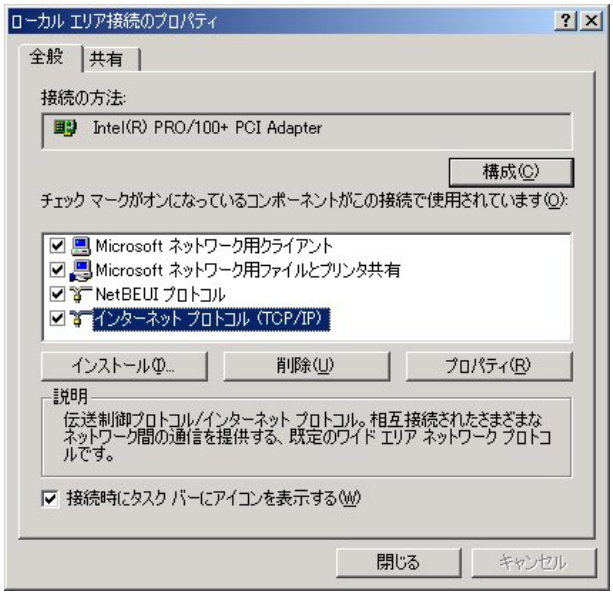
4 最後に OK ボタンをクリックするとコンピューターが再起動します。再起動後に、XR-410 の設定画面へのログインが可能になります。

II. Windows 2000のネットワーク設定

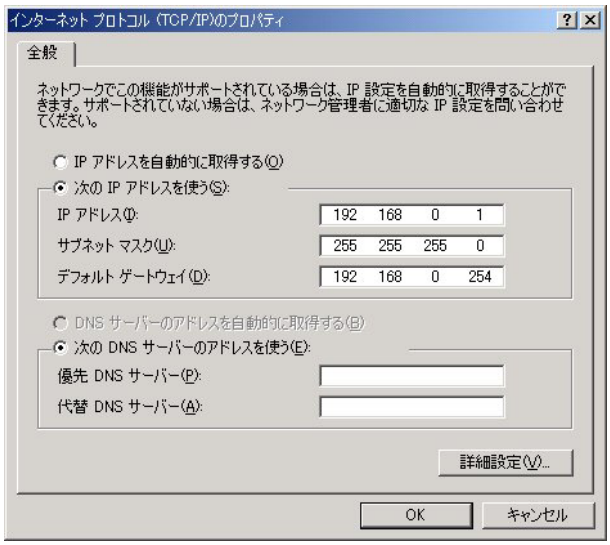
ここではWindows2000が搭載されたコンピューターのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワークとダイヤルアップ接続」から、「ローカル接続」を開きます。

2 画面が開いたら、「インターネットプロトコル(TCP/IP)」のプロパティを開きます。



3 「全般」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



4 最後にOKボタンをクリックして設定完了です。
これでXR-410へのログインの準備が整いました。

III. Windows XP のネットワーク設定

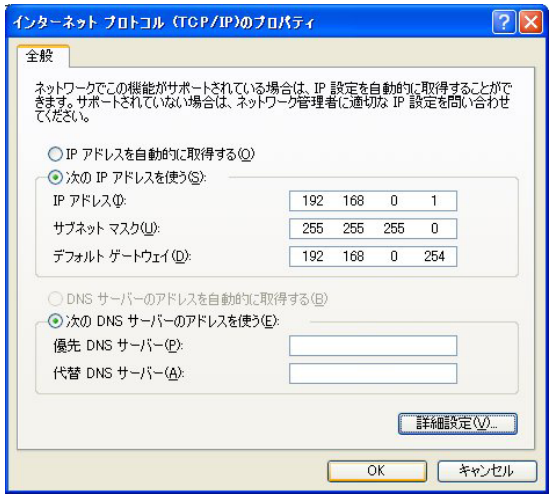
ここではWindowsXPが搭載されたコンピューターのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコル(TCP/IP)」を選択して「プロパティ」ボタンをクリックします。

4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



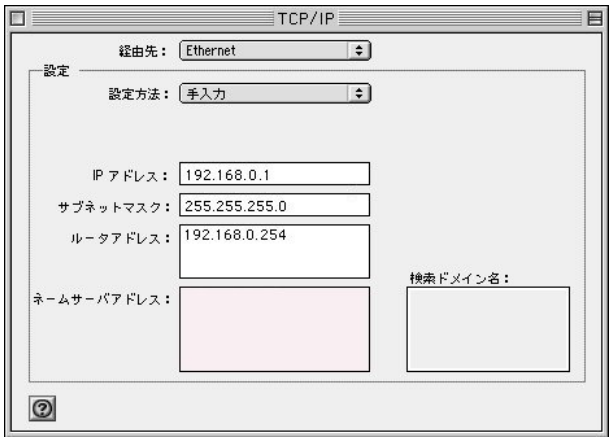
5 最後にOKボタンをクリックして設定完了です。
これでXR-410へのログインの準備が整いました。

IV. Macintoshのネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

1 「アップルメニュー」から「コントロールパネル」→「TCP/IP」を開きます。

2 経由先を「Ethernet」、設定方法を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」



3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これでXR-410へログインする準備が整いました。

V. IP アドレスの確認と再取得

◆Windows95/98/Me の場合

1 「スタート」→「ファイル名を指定して実行」を開きます。

2 名前欄に、”winipcfg” というコマンドを入力して「OK」をクリックしてください。

3 「IP 設定」画面が開きます。リストから、パソコンに装着されている LAN ボード等を選び、「詳細」をクリックしてください。その LAN ボードに割り当てられた IP アドレス等の情報が表示されます。

4 「IP 設定」画面で「全て開放」をクリックすると、現在の IP 設定がクリアされます。引き続いて「すべて書き換え」をクリックすると、IP 設定を再取得します。

◆WindowsNT3.51/4.0/2000 の場合

1 「スタート」→「プログラム」→「アクセサリ」→「コマンドプロンプト」を開きます。

2 以下のコマンドを入力すると、現在の IP 設定がウィンドウ内に表示されます。

```
c:\>ipconfig /all
```

3 IP 設定のクリアと再取得をするには以下のコマンドを入力してください。

```
c:\>ipconfig /release   (IP 設定のクリア)
c:\>ipconfig /renew     (IP 設定の再取得)
```

◆Macintosh の場合

IP 設定のクリア / 再取得をコマンド等でおこなうことはできませんので、Macintosh 本体を再起動してください。

XR-410 の IP アドレス・DHCP サーバ設定を変更したときは、必ず IP 設定の再取得をするようにしてください。

第4章

設定画面へのログイン

設定画面へのログイン方法

1 各種ブラウザを開きます。

2 ブラウザから設定画面にアクセスします。

ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。

http://192.168.0.254:880/

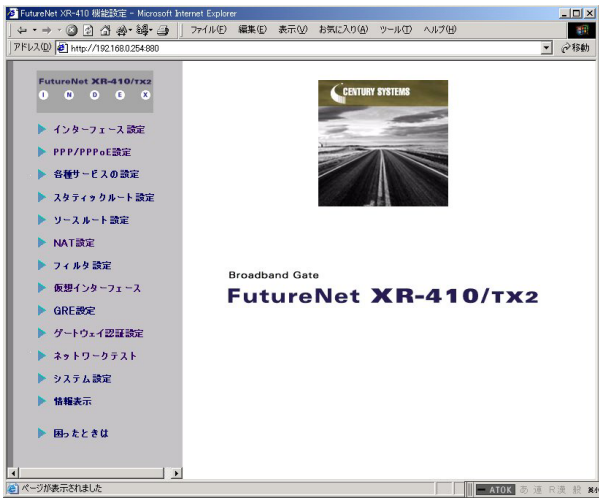
「192.168.0.254」は、Ether0 ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。**設定画面のポート番号 880 は変更することができません。**

3 次のような認証ダイアログが表示されます。

4 ダイアログ画面にパスワードを入力します。

工場出荷設定のユーザー名とパスワードはともに「admin」です。ユーザー名・パスワードを変更している場合は、それにあわせてユーザー名・パスワードを入力します。

5 ブラウザ設定画面が表示されます。



工場出荷時の設定では Ether0 ポート以外のインターフェースではすべてステートフルパケットインスペクションが有効になっています。そのため Ether0 ポート以外のインターフェースからは設定画面にアクセスできません。

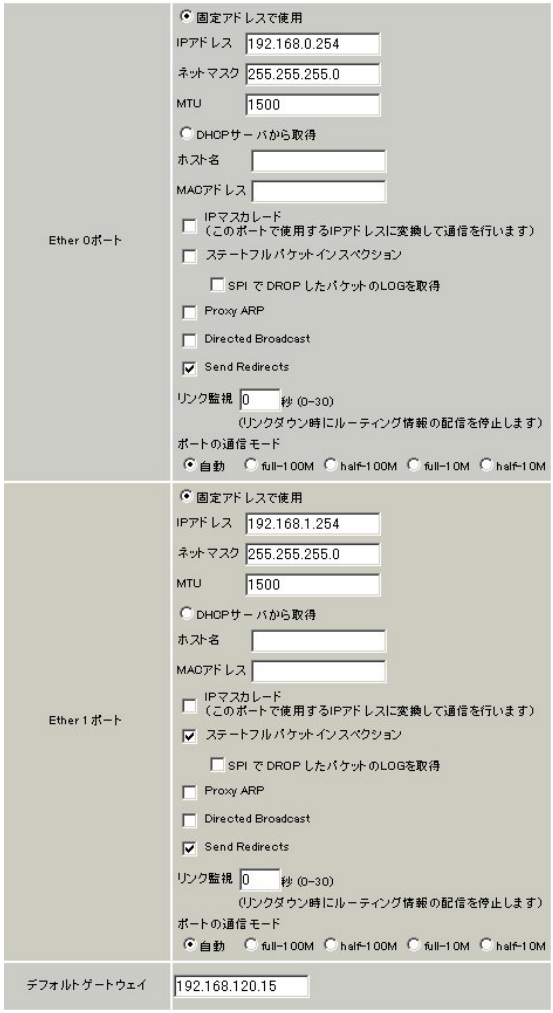
Ether0 ポート以外のインターフェースから設定できるようにするには、それぞれのインターフェースのステートフルパケットインスペクションを無効にするか、パケットフィルタリング設定をおこなってください。

第5章

インターフェース設定

1.Ethernet ポートの設定

ここでは本装置の各 Ethernet ポートの設定をおこないます。
Web 設定画面「インターフェース設定」->「Ethernet ポートの設定」をクリックして以下の画面で設定します。



各インターフェースについて、それぞれ必要な情報を入力します。

○ IP アドレスが固定割り当ての場合は「固定アドレスで使用」にチェックして、IP アドレスとネットマスクを入力します。

○ IP アドレスが DHCP で割り当ての場合は「DHCP から取得」にチェックして、必要であればホストネームと MAC アドレスを設定します。

MAC アドレスの入力例
00:11:22:33:44:55（コロンで区切ります）

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、ここの値を変更することで回避できます。通常は初期設定の 1500byte のままでかまいません。

○ IP マスカレード
チェックを入れると、その Ethernet ポートで IP マスカレードされます。

○ステートフルパケットインスペクション
チェックを入れると、その Ethernet ポートでステートフルパケットインスペクション(SPI)が適用されます。

○ SPI で DROP したパケットの LOG を取得
チェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 25 章「補足：フィルタのログ出力内容について」をご覧下さい。

○ Proxy ARP
ProxyARP を使う場合はチェックします。

○ Directed Broadcast
チェックを入れると、そのインタフェースにおいて DirectedBroadcast の転送を許可します。

Directed Broeadcast
IP アドレスのホスト部がすべて 1 のアドレスのことです。
ex.192.168.0.0/24 の Directed Broadcast は 192.168.0.255 です。

○ Send Redirects
チェックを入れると、そのインタフェースにおいて ICMP Redirects を送出します。

ICMP Redirects
他に適切な経路があることを通知する ICMP パケットのことです。

Ⅰ.Ethernet ポートの設定

○リンク監視
チェックを入れると、Ethernet ポートのリンク状態の監視を定期的に行います。OSPF の使用時にリンクのダウンを検知した場合、そのインタフェースに関連付けられたルーティング情報の配信を停止します。再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。監視間隔は 1～30 秒の間で設定できます。また、0 を設定するとリンク監視を行いません。

○ポートの通信モード
各 Ether ポートの通信速度・方式を選択します。工場出荷設定では「自動」(オートネゴシエーション)となっていますが、通信速度・方式を固定できますので、必要に応じて選択します。

○デフォルトゲートウェイ
本装置のデフォルトルートとなる IP アドレスを入力してください。

入力が終わりましたら「設定の保存」をクリックして設定完了です。設定はすぐに反映されます。

XR-410 のインタフェースのアドレスを変更した後は設定が直ちに反映されます。設定画面にアクセスしているホストやその他クライアントの IP アドレス等も XR の設定にあわせて変更し、変更後の IP アドレスで設定画面に再ログインしてください。

11.Ethernetポートの設定について

[ステートフルパケットインスペクション]

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能とも言えるものです。
通常はWANからのアクセスを全て遮断し、WAN方向へのパケットに対応するLAN方向へのパケット(WANからの戻りパケット)に対してのみポートを開放します。これにより、自動的にWANからの不要なアクセスを制御でき、簡単な設定でより高度な安全性を保つことができます。

ステートフルパケットインスペクション機能を有効にすると、そのインターフェースへのアクセスは一切不可能となります。ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります(第25章参照)。

[PPPoE接続時のEthernetポート設定]

PPPoE回線に接続するEthernetポートの設定については、実際には使用しない、ダミーのプライベートIPアドレスを設定しておきます。

XR-410がPPPoEで接続する場合には”ppp”という論理インターフェースを自動的に生成し、このppp論理インターフェースを使ってPPPoE接続をおこなうためです。

物理的なEthernetポートとは独立して動作していますので、「DHCPサーバから取得」の設定やグローバルIPアドレスの設定はしません。PPPoEに接続しているインターフェースでこれらの設定をおこなうと、正常に動作しなくなる場合があります。

[IPsec通信時のEthernetポート設定]

XR-410をIPsecゲートウェイとして使う場合は、Ethernetポートの設定に注意してください。

IPsec通信をおこなう相手側のネットワークと同じネットワークのアドレスがXR-410のEthernetポートに設定されていると、正常にIPsec通信がおこなえません。

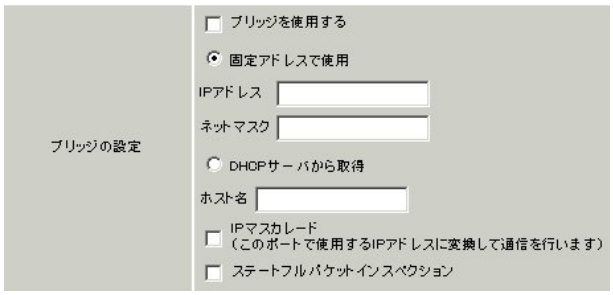
たとえば、IPsec通信をおこなう相手側のネットワークが192.168.1.0/24で、且つ、XR-410のEther1ポートに192.168.1.254が設定されていると、正常にIPsec通信がおこなえません。

このような場合はXR-410のEthernetポートのIPアドレスを、別のネットワークに属するIPアドレスに設定し直してください。

III.Ethernet ブリッジの設定

ここでは本装置をブリッジとして運用するための設定をおこないます。

Web 設定画面「インターフェース設定」->「Ethernet ブリッジの設定」をクリックして、以下の画面で設定します。



○「ブリッジを使用する」にチェックすると、本装置の Ethernet ポートはブリッジインターフェースとなります。

○「固定アドレスで使用」
ブリッジインターフェースの IP アドレスを固定アドレスで設定する場合はこちらをチェックして、IP アドレスとネットマスクを入力します。

○「DHCP サーバから取得」
ブリッジインターフェースの IP アドレスを DHCP から取得する場合はこちらをチェックします。必要であればホスト名を入力します。

○ IP マスカレード
チェックすると、ブリッジインターフェースから出ていくパケットについて IP マスカレードされます。

○ステートフルパケットインスペクション
チェックを入れたポートから出ていくパケットについて、ステートフルパケットインスペクションが適用されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。設定はすぐに反映されます。

IV. 通常接続(CATV など)での接続設定例

ここでは NAT を使った CATV インターネット接続の設定について説明します。
CATV のほかにも、Yahoo!BB などルータ型 ADSL モデムを用いて接続する場合もこちらをご覧ください。

接続環境

・WAN 側 IP アドレスは DHCP で自動取得
・LAN 側 IP アドレスは工場出荷設定のまま
・Ether0 ポートを LAN、Ether1 ポートを WAN に接続する

設定方法

「インターフェース設定」画面を開きます。
○ Ether0 ポート
・「固定アドレスで使用」にチェック
・IP アドレス「192.168.0.254」
・サブネットマスク「255.255.255.0」
・「IP マスカレード」「ステートフルパケットインスペクション」には**チェックしません**。

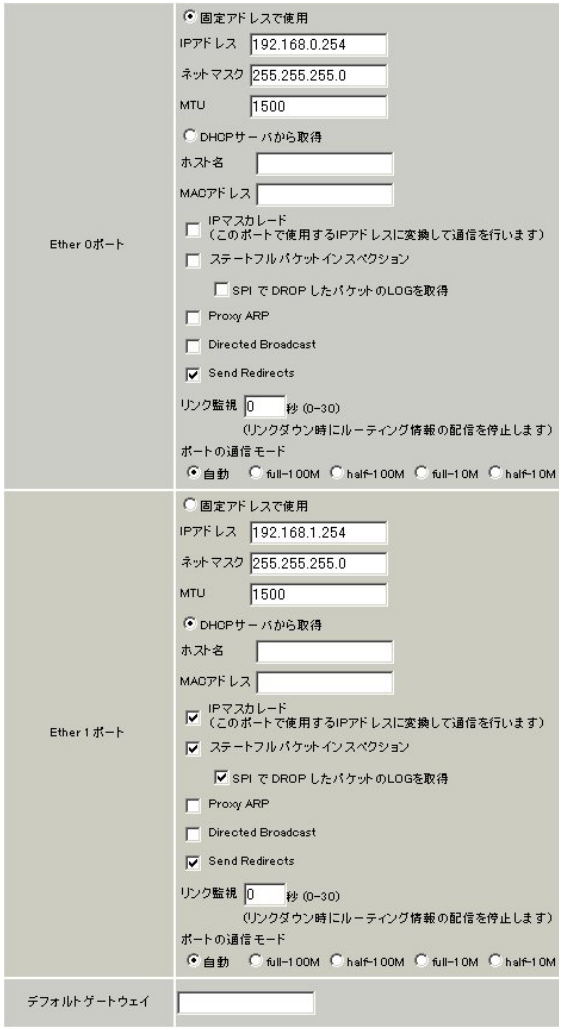
○ Ether1 ポート
・「DHCP から取得」にチェック
・必要であれば「ホスト名」を入力
・任意で MAC アドレスを指定することもできます。
　＜入力例＞　***00:80:6d:49:ff:ff***
・「IP マスカレード」にチェック
・任意で「ステートフルパケットインスペクション」にチェックしてください。ステートフルパケットインスペクション機能を使わない場合は、詳細なパケットフィルタの設定をおこなってください。

○その他項目については任意で設定してください。

○デフォルトルート
入力しません。

WAN 側ポートを固定アドレスで接続する場合は、IP アドレス・ネットマスク・デフォルトルートについて入力します。ルータタイプの ADSL モデムに接続する場合などは、ルータモデムの IP アドレスがデフォルトルートとなります。

画面での入力例



Ether0 ポートの設定を変更したときは、必ず各コンピューターの IP アドレス設定も変更してください。

また、各コンピューターを DHCP クライアントとして使用する場合は、DHCP サーバ機能の設定をおこなう必要があります。DHCP サーバ機能については**第 11 章**をご覧ください。

V. ローカルルータ設定

ここでは本装置をローカルルータとして使うための設定について説明します。

接続環境

・Ether0 側 IP アドレスは「192.168.0.254]
・Ether0 側サブネットマスクは「255.255.255.0」
・Ether1 側 IP アドレスは「192.168.1.254]
・Ether1 側サブネットマスクは「255.255.255.0」

設定方法

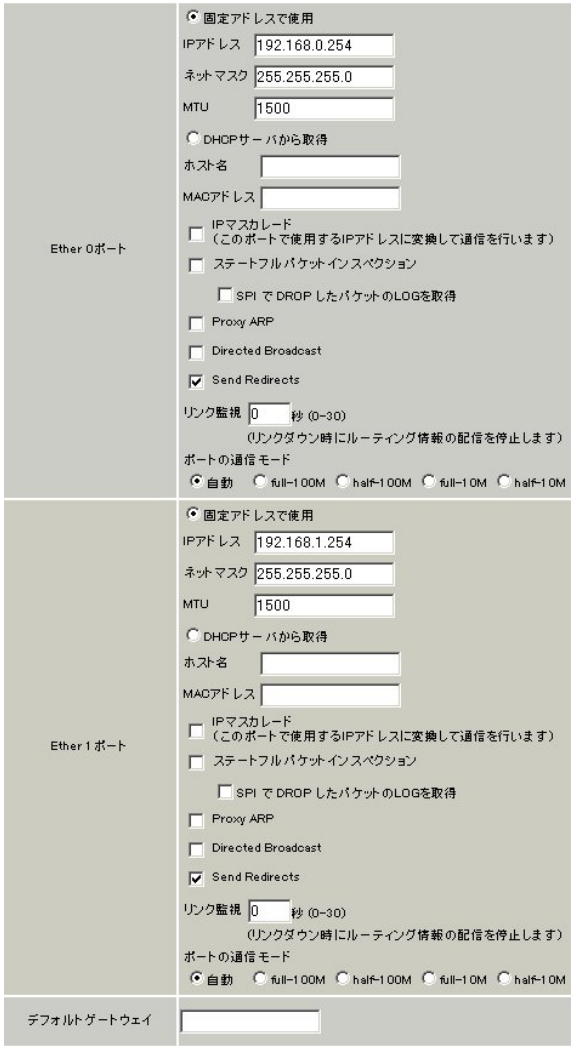
「インターフェース設定」画面を開きます。
○ Ether0 ポート
・「固定アドレスで使用」にチェック
・IP アドレス「192.168.0.254」
・サブネットマスク「255.255.255.0」
・「IP マスカレード」「ステートフルパケットインスペクション」には**チェックしません**。

○ Ether1 ポート
・「固定アドレスで使用」にチェック
・IP アドレス「192.168.1.254」
・サブネットマスク「255.255.255.0」
・「IP マスカレード」「ステートフルパケットインスペクション」には**チェックしません**。

○ポートの通信モード
任意で選択してください。

○デフォルトルート
必要に応じて指定してください。

画面での入力例



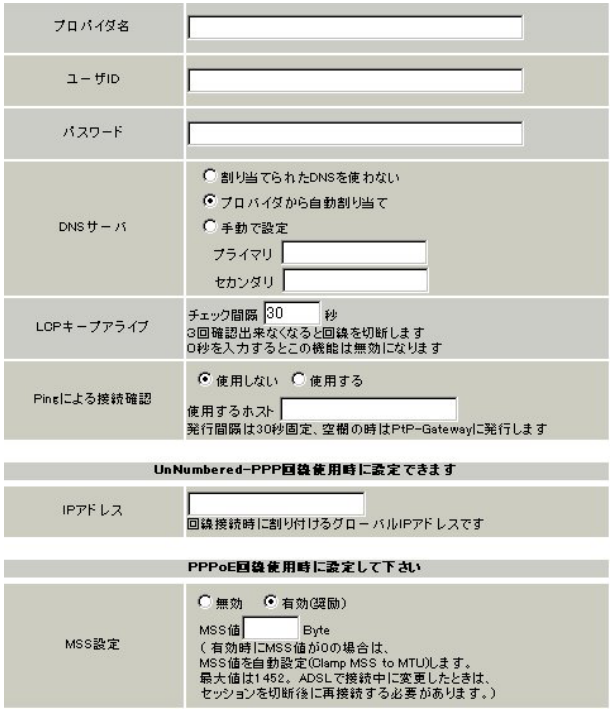
第 6 章

PPPoE 設定

Ⅰ．PPPoE の接続先設定

Web 設定画面「PPP/PPPoE 設定」をクリックします。

はじめに、接続先の設定（ISP のアカウント設定）をおこないます。「接続先設定」1～5 のいずれかをクリックします(5つまで設定を保存しておくことがきます)。



○プロバイダ名
接続するプロバイダ名を入力します。任意に入力できますが、半角英数字のみ使用できます。

○ユーザー ID
プロバイダから指定されたユーザー ID を入力してください。

○ パスワード
プロバイダから指定された接続パスワードを入力してください。

原則として「 ’ 」「(」「)」「｜」「\」等の特殊記号については使用できませんが、入力が必要な場合は該当文字の直前に「\」を付けて入力してください。

<例>
abc(def)g ’ h → abc\(def\)g\ ’ h

○ DNS サーバ
特に指定のない場合は「プロバイダから自動割り当て」をチェックします。
指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。
プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられた DNS を使わない」をチェックします。この場合は、LAN 側の各ホストに DNS サーバのアドレスをそれぞれ設定しておく必要があります。

○ LCP キープアライブ
キープアライブのための LCP echo パケットを送出する間隔を指定します。設定した間隔で LCP echo パケットを 3 回送出して reply を検出しなかったときに、XR-410 が PPPoE セッションをクローズします。「0」を指定すると、LCP キープアライブ機能は無効となります。

○ Ping による接続確認
回線によっては、LCP echo を使ったキープアライブを使うことができないことがあります。その場合は、Ping を使ったキープアライブを使用します。「使用するホスト」欄には、Ping の宛先ホストを指定します。空欄にした場合は P-t-P Gateway 宛に Ping を送出します。

Ⅰ．PPPoE の接続先設定

○ IP アドレス
固定 IP アドレスを割り当てられる接続の場合(unnumbered 接続を含む)、ここにプロバイダから割り当てられた IP アドレスを設定します。IP アドレスを自動的に割り当てられる形態での接続の場合は、ここにはなにも入力しないでください。

○ MSS 設定
「有効」を選択すると、XR-410 が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。最大値は 1452 バイトです。
「0」にすると最大 1414byte に自動調整します。
特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします(それ以外では正常にアクセスできなくなる場合があります)。

MSS 設定項目以下は設定しません。

最後に「設定」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

LAN 側の設定(IP アドレスや DHCP サーバ機能など)を変更する場合は、それぞれの設定ページで変更してください。

11．PPPoE の接続設定と回線の接続 / 切断

Web 設定画面「PPP/PPPoE 接続設定」をクリックし、右画面の「接続設定」をクリックして、以下の画面から設定します。

接続設定

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

○接続ポート
どのポートを使って接続するかを選択します。
PPPoE 接続では、いずれかの Ethernet ポートを選択します。

○接続形態
「手動接続」PPPoE(PPP)の接続 / 切断を手動で切り替えます。
「常時接続」XR-410 が起動すると自動的に PPPoE 接続を開始します。

○ IP マスカレード
PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 25 章「補足：フィルタのログ出力内容について」をご覧下さい。

○デフォルトルートの設定
「有効」を選択すると、PPPoE 接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、PPPoE 接続で通知されるものに置き換えられます。

「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。**通常は「有効」設定にしておきます。**

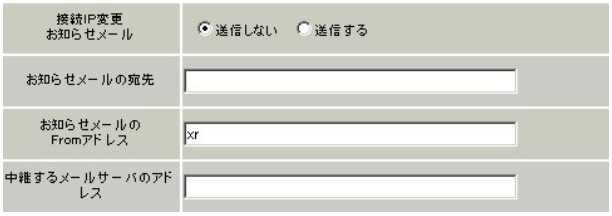
この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

III. その他の接続設定

接続 IP 変更お知らせメール機能

IP アドレスを自動的に割り当てられる方式で PPPoE 接続する場合、接続のたびに割り当てられる IP アドレスが変わってしまうことがあります。
この機能を使うと、IP アドレスが変わったときに、その IP アドレスを任意のメールアドレスにメールで通知することができるようになります。

以下の箇所で設定します。



○接続 IP 変更お知らせメール
お知らせメール機能を使う場合は、「送信する」を選択します。

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス
お知らせメールのヘッダに含まれる、”From ”項目を任意で設定することができます。

○中継するメールサーバのアドレス
お知らせメールを中継する任意のメールサーバを設定できます。IP アドレス、ドメイン名のどちらでも設定できます。
ただしドメイン名で指定するときは、下記の記述で設定してください。

＜入力形式＞　**@＜ドメイン名＞**
＜入力例＞　　@mail.xxxxxx.co.jp

IV. 副回線とバックアップ回線

PPPoE 接続では、「副回線接続」設定と「バックアップ回線接続」設定ができます。

[副回線接続]

主回線が何らかの理由で切断されてしまったときに、自動的に副回線設定での接続に切り替えて、接続を維持することができます。また主回線が再度接続されると、自動的に副回線から主回線の接続に戻ります。

主回線から副回線の接続に切り替わっても、NAT 設定やパケットフィルタ設定、ルーティング設定等の全ての設定が、そのまま副回線接続にも引き継がれます。

回線状態の確認は、セッションキープアライブ機能を用います。

[バックアップ回線接続]

副回線接続と同様に、主回線がダウンしたときに、自動的に回線を切り替えて接続を維持しようとします。

ただし副回線接続と異なり、NAT 設定やパケットフィルタ設定等は、主回線用の設定とは別に設定しなければなりません。

これにより、主回線接続時とバックアップ回線接続時とでセキュリティレベルを変更したり、回線品質にあった帯域制御などを個別に設定する、といったことができるようになります。

回線状態の確認は、ping または OSPF を用います。OSPF については、「第 21 章ダイナミックルーティング」をご覧ください。

副回線設定

PPPoE 接続設定画面の「副回線使用時に設定して下さい」欄で設定します。

○副回線の使用
副回線を利用する場合は「有効」を選択します。

○接続先の選択
副回線接続で利用する接続先設定を選択します。

○接続ポート
副回線を接続しているインタフェースを選択します。

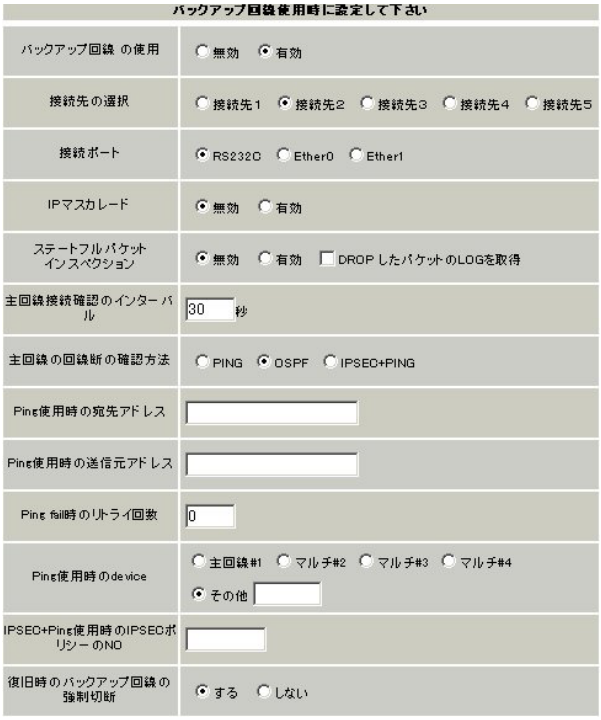
上記 3 項目以外の接続設定は、すべてそのまま引き継がれます。

副回線での自動接続機能は、「接続設定」で「常時接続」に設定してある場合のみ有効です。
また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

IV. 副回線とバックアップ回線

バックアップ回線設定

PPPoE 接続設定画面の「バックアップ回線使用時に設定して下さい」欄で設定します。



○バックアップ回線 の使用
バックアップ回線を利用する場合は「有効」を選択します。

○接続先の選択
バックアップ回線接続で利用する接続先設定を選択します。

○接続ポート
バックアップ回線で使用するインタフェースを選択します。

○ IP マスカレード
バックアップ回線接続時の IP マスカレードの動作を選択します。

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 25 章「補足：フィルタのログ出力内容について」をご覧下さい。

○主回線接続確認のインターバル
主回線接続の確認ためにパケットを送出する間隔を設定します。

○主回線の回線断の確認方法
主回線の回線断を確認する方法を選択します。「PING」は ping パケットにより、「OSPF」は OSPF の Hello パケットにより、「IPSEC+PING」は IPSEC 上での ping により、回線の切断を確認します。

○ Ping 使用時の宛先アドレス
回線断の確認方法で ping を選択したときの、ping パケットのあて先 IP アドレスを設定します。ここから ping の Reply が帰ってこなかった場合に、バックアップ回線接続に切り替わります。

OSPF の場合は、OSPF 設定画面「OSPF 機能設定」の「バックアップ切り替え監視対象 Remote Router-ID 設定」で設定した IP アドレスに対して接続確認をおこないます。

○ Ping 使用時の送信元アドレス
回線断の確認方法で「IPSEC+PING」を選択したときの、ping パケットの送信元 IP アドレスを設定できます。

○ Ping fail 時のリトライ回数
pingのリプライがないときに何回リトライするかを指定します。

IV. 副回線とバックアップ回線

○ Ping 使用時の device
ping を使用する際の、ping を発行する回線(インタフェース)を選択します。「その他」を選択して、インタフェース名を直接指定もできます。

○ IPSEC ＋ PING 使用時の IPSEC ポリシーの NO
IPSEC+PING で回線断を確認するときは必ず、使用する IPsec ポリシーの設定番号を指定します。
IPsec 設定については「第 12 章 IPsec 設定」や IPsec 設定ガイドをご覧下さい。

○復旧時のバックアップ回線の強制切断
主回線の接続が復帰したときに、バックアップ回線を強制切断させるときに「する」を選択します。「しない」を選択すると、主回線の接続が復帰しても、バックアップ回線接続の設定に従ってバックアップ回線の接続を維持します。

このほか、NAT 設定・パケットフィルタ設定・ルーティング設定など、バックアップ回線接続時のための各種設定を別途行なってください。

バックアップ回線接続機能は、「接続接定」で「常時接続」に設定してある場合のみ有効です。また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

接続変更お知らせメール機能

バックアップ回線で接続したときに、それを電子メールによって通知させることができます。

以下の箇所で設定します。

○接続お知らせメール
お知らせメール機能を使う場合は、「有効」を選択します。

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス
お知らせメールのヘッダに含まれる、”From ”項目を任意で設定することができます。

○中継するメールサーバのアドレス
お知らせメールを中継する任意のメールサーバを設定できます。IP アドレス、ドメイン名のどちらでも設定できます。
ただしドメイン名で指定するときは、下記の記述で設定してください。

＜入力形式＞　**@ ＜ドメイン名＞**
＜入力例＞　　@mail.xxxxxx.co.jp

V.PPPoE 特殊オプション設定について

PPPoE 接続時には、特殊なオプション設定を使うことができます。

①回線接続時に前回の PPPoE セッションの PADT を強制送出する。

②非接続 Session の IPv4Packet 受信時に PADT を強制送出する。

③非接続 Session の LCP-EchoReqest 受信時に PADT を強制送出する。

①の動作について

XR 側が回線断と判断していても網側が回線断と判断していない状況下において、XR 側から強制的に PADT を送出してセッションの終了を網側に認識させます。その後、XR 側から再接続を行います。

②、③の動作について

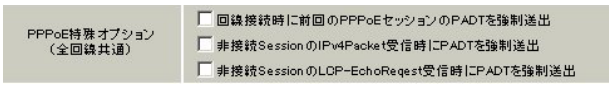
XR が LCP キープアライブにより断を検知しても網側が断と判断していない状況下において、
網側から
- IPv4 パケット
- LCP エコーリクエスト

のいずれかを XR が受信すると、XR が PADT を送出してセッションの終了を網側に認識させます。
その後、XR 側から再接続を行います。

PADT ＝ PPPoE Active Discovery Terminate の略。PPPoE セッションが終了したことを示すパケットです。これにより、PADT を受信した側で該当する PPPoE セッションを終了させます。

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。



使用したい特殊オプションごとに、チェックボックスにチェックを付けてください。

PPPoE 回線接続中に設定を変更したときは、PPPoE を再接続する必要があります。

第7章

RS-232ポートを使った接続
(リモートアクセス機能)

第 7 章　RS-232 ポートを使った接続(リモートアクセス機能)

Ⅰ．XR-410 とアナログモデム /TA の接続

XR-410 は、RS-232 ポートを搭載しています。これらの各ポートにアナログモデムやターミナルアダプタを接続し、XR-410 の PPP 接続機能を使うことでリモートアクセスが可能となります。

また XR-410 の副回線接続機能で、PPP 接続を副回線として設定しておくと、リモートアクセスを障害時のバックアップ回線として使うこともできます。

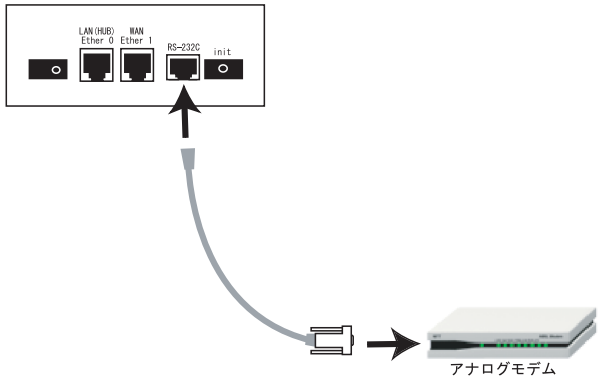
◆アナログモデム /TA の接続

1 XR-410 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

2 変換アダプタのコネクタを、アナログモデムのシリアルポートに接続してください。モデムのコネクタが 25 ピンタイプの場合は別途、変換コネクタをご用意ください。

3 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図

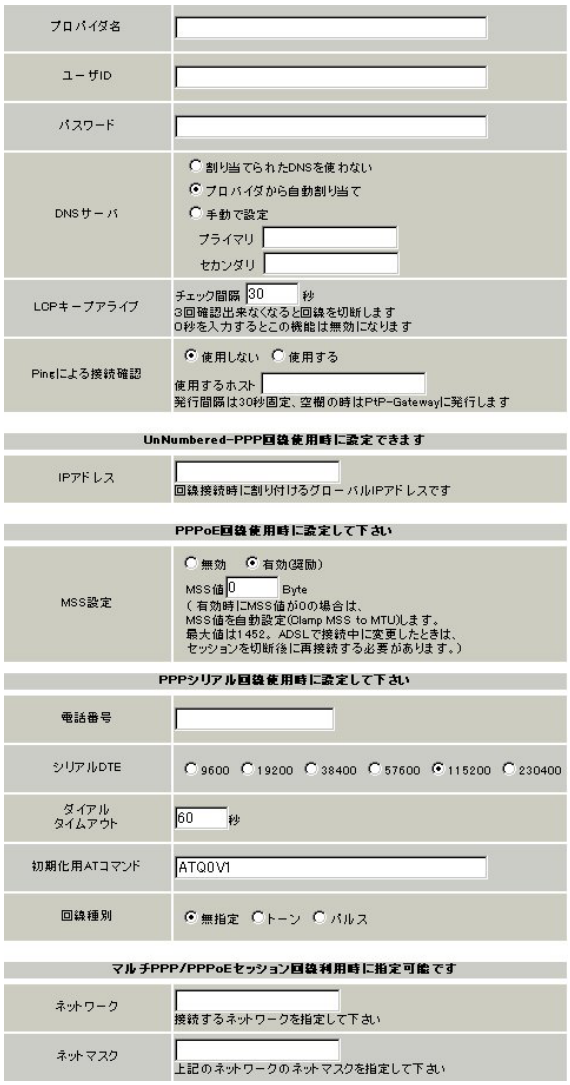


II．リモートアクセス回線の接続先設定

PPP(リモートアクセス)接続の接続先設定を行ないます。以下の手順で設定してください。

Web 設定画面「PPP/PPPoE 設定」をクリックして接続先の設定をおこないます。

右画面上部「接続先設定」１～５のいずれかをクリックします(5つまで設定を保存しておくことができます)。



○プロバイダ名
接続するプロバイダ名を入力します任意に入力できますが、半角英数字のみ使用できます。

○ユーザー ID
プロバイダから指定されたユーザー ID を入力してください。

○パスワード
プロバイダから指定された接続パスワードを入力してください。

原則として「 ’」「(」「)」「｜」「\」等の特殊文字については使用できませんが、入力が必要な場合は該当文字の直前に「\」を付けて入力してください。

<例>　abc(def)g ’ h → abc\(def\)g\ ’ h

○DNS サーバ
特に指定のない場合は「プロバイダから自動割り当て」をチェックします。指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。

プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられた DNS を使わない」をチェックします。この場合は、LAN 側の各ホストに DNS サーバのアドレスをそれぞれ設定しておく必要があります。

○LCP キープアライブ
○ping による接続確認
○IP アドレス
○MSS 設定
上記項目は、リモートアクセス接続の場合は設定の必要はありません。

○電話番号
アクセス先の電話番号を入力します。
市外局番から入力してください。

11．リモートアクセス回線の接続先設定

〇ダイアルタイムアウト
アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

〇シリアル DTE
XR-410 とモデム /TA 間の DTE 速度を選択します。
工場出荷値は 115200bps です。

〇初期化用 AT コマンド
モデム /TA によっては、発信するときに初期化が必要なものもあります。その際のコマンドをここに入力します。

〇回線種別
回線のダイアル方法を選択します。

最後に「設定の保存」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

続いて PPP の接続設定を行ないます。

III．リモートアクセス回線の接続と切断

接続先設定に続いて、リモートアクセス接続のために接続設定をおこないます。

Web 設定画面「PPP/PPPoE 接続設定」をクリックします。右画面の「接続設定」をクリックして、以下の画面から設定します。

接続設定

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

○接続ポート
どのポートを使って接続するかを選択します。
リモートアクセス接続では「RS232C」ポートを選択します。

○接続形態
「手動接続」リモートアクセスの接続 / 切断を手動で切り替えます。
「常時接続」XR-410 が起動すると自動的にリモートアクセス接続を開始します。

○ IP マスカレード
リモートアクセス接続時に IP マスカレードを有効にするかどうかを選択します。unnumbered 接続時以外は、「有効」を選択してください。

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 25 章「補足：フィルタのログ出力内容について」をご覧下さい。

○デフォルトルートの設定
「有効」を選択すると、リモートアクセス接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、リモートアクセス接続で通知されるものに置き換えられます。

「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。**特に必要のない限り「有効」設定にしておきます。**

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

Ⅳ．副回線接続とバックアップ回線接続

リモートアクセス接続についても、PPPoE 接続と同様に、副回線接続設定とバックアップ回線接続設定が可能です。

設定方法については、第 6 章をご覧ください。

第8章

複数アカウント同時接続設定

複数アカウント同時接続の設定

XR-410 シリーズは、同時に複数の PPPoE 接続をおこなうことができます。以下のような運用が可能です。

・NTT 東西が提供している B フレッツサービスで、インターネットとフレッツ・スクエアに同時に接続する(注)
・フレッツ ADSL での接続と、ISDN 接続(リモートアクセス)を同時におこなう

(注)NTT 西日本の提供するフレッツスクエアは NTT 東日本提供のものとはネットワーク構造がことなるため、B フレッツとの同時接続運用はできません。

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。
XR-410 のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。なお、以下の項目については主回線では設定できますが、マルチ接続（#2 ～ #4）では設定できませんので、ご注意下さい。

・デフォルトルートとして指定する
・副回線を指定する
・接続 IP アドレス変更のお知らせメールを送る

マルチ PPPoE セッションを利用する場合のルーティングは宛先ネットワークアドレスによって切り替えます。したがって、フレッツ・スクウェアやフレッツ・オフィスのように特定の IP アドレス体系で提供されるサービスをインターネット接続と同時に利用する場合でも、アクセスする PC 側の設定を変更する必要はありません。

ただし、マルチリンクには対応していませんので、帯域を広げる目的で利用することはできません。
また XR-410 のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインターフェースがルーティングの対象となります。したがいまして、それぞれのインターフェースにステートフルパケットインスペクション、又はフィルタリング設定をしてください。

またマルチ接続側（主回線ではない側）は**フレッツスクエアのように閉じた空間を想定している**ので、工場出荷設定ではステートフルパケットインスペクションは無効となっています。必要に応じてステートフルパケットインスペクション等の設定をして使用してください。

この機能を利用する場合は以下のステップに従って設定して下さい。

STEP 1 主接続の接続先設定

１つ目のプロバイダの接続設定をおこないます。ここで設定した接続を主接続とします。

Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。詳しい設定方法は、第 6 章をご覧ください。

複数アカウント同時接続の設定

STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。設定方法については、**第 6 章**をご参照ください。

さらに設定画面最下部にある下図の部分で、マルチ接続を使ってアクセスしたい先のネットワークアドレスとネットマスクを指定します。

マルチPPP/PPPoEセッション回線利用時に指定可能です	
ネットワーク	接続するネットワークを指定して下さい
ネットマスク	上記のネットワークのネットマスクを指定して下さい

例えば

○ネットワークアドレスに「172.26.0.0」

○ネットマスクに「255.255.0.0」

と指定すると、172.26.0.0/16 のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

別途「スタティックルート設定」でマルチ接続を使う経路を登録することもできます。

<u>このどちらも設定しない場合はすべてのアクセスが、主接続を使うことになります。</u>

最後に「設定の保存」をクリックして接続先設定は完了です。

STEP 3 PPPoE 接続の設定

複数同時接続のための接続設定をおこないます。主接続とマルチ接続それぞれについて接続設定をおこないます。

「PPP/PPPoE 設定」->「接続設定」を開きます。

[主接続用の接続設定]

以下の部分で設定します。

回線状態	回線は接続されていません
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
接続形態	◉手動接続 ○常時接続
IPマスカレード	○無効 ◉有効
ステートフルパケットインスペクション	○無効 ◉有効 □DROP したパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効

○接続先の選択

主接続用の設定を選択します。

○接続先ポート

主接続で使用する、XR-410 のインタフェースを選択します。

○接続形態

常時接続の回線を利用する場合は通常、「常時接続」を選択します。手動接続を選択した場合は、同画面最下部のボタンで接続・切断の操作をおこなってください。

○ IP マスカレード

通常は「有効」を選択します。

LAN 側をグローバル IP で運用している場合は「無効」を選択します。

○ステートフルパケットインスペクション

任意で選択します。

○デフォルトルート

「有効」を選択します。

○接続 IP 変更お知らせメール

任意で設定します。

続いてマルチ接続用の接続設定をおこないます。

複数アカウント同時接続の設定

[マルチ接続用の設定]

以下の部分で設定します。

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい	
マルチ接続 #2	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 □DROP したパケットのLOGを取得
マルチ接続 #3	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 □DROP したパケットのLOGを取得
マルチ接続 #4	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 □DROP したパケットのLOGを取得

○マルチ接続 #2 ～ #4

マルチ PPPoE セッション用の回線として使うものに「有効」を選択します。

○接続先の選択

マルチ接続用の接続先設定を選択します。

○接続ポート

マルチ接続で使用する、XR-410 のインタフェースを選択します。B フレッツ回線で複数の同時接続をおこなう場合は、主接続の設定と同じインタフェースを選択します。

○ IP マスカレード

通常は「有効」を選択します。
LAN 側をグローバル IP で運用している場合は「無効」を選択します。

○ステートフルパケットインスペクション

任意で選択します。

マルチ接続設定は 3 つまで設定可能です(最大 4 セッションの同時接続が可能)。

複数アカウント同時接続の設定

STEP 4　PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。

PPPoE の接続状態は、接続設定画面上部の「回線状態」に赤文字で表示されます。

接続に成功した場合:

主回線で接続しています。
マルチセッション回線 1 で接続しています。

接続できていない場合:

主回線で接続を試みています。
マルチセッション回線 1 で接続を試みています。

などと表示されます。

PPPoE 接続に成功したあとは、STEP 2 の設定、「スタティックルート設定」もしくは「ソースルート設定」にしたがって接続を振り分けられてアクセスできます。

第9章

各種サービスの設定

各種サービス設定

Web 設定画面「各種サービスの起動・停止・設定」をクリックすると、以下の画面が表示されます。

ここでは

・各種サービスの設定
・各種サービスの起動と停止
・サービスの稼働状況の確認

をおこないます。

サービスの設定

それぞれのサービスの設定をおこなうには、画面中の各サービス名をクリックしてください。そのサービスの設定画面が表示されます。
それぞれの設定方法については、以下のページを参照してください。

DNS サーバ機能

DHCP サーバ / リレー機能

IPsec 機能

UPnP 機能

ダイナミックルーティング機能

SYSLOG 機能

帯域制御(QoS)機能

攻撃検出機能

SNMP エージェント機能

NTP サービス

VRRP サービス

アクセスサーバ機能

サービスの起動と停止

それぞれのサービスを起動・停止するときは、それぞれのサービス項目で、「停止」か「起動」を選択して画面最下部にある「動作変更」ボタンをクリックすることで、サービスの稼働状態が変更されます。また、サービスの稼働状態は、各項目の右側に表示されます。

第 10 章

DNS リレー / キャッシュ機能

Ⅰ. DNS キャッシュ機能の概要

◆DNS リレー機能

通常インターネットにアクセスする場合は、各ホストが DNS サーバに対して直接名前解決の問い合わせをおこないます。

しかし DNS リレー機能を使うと、ホストの名前解決要求を XR-410 が受けて、XR-410 が DNS サーバに名前解決要求を中継します。

これにより、各ホストの DNS サーバ設定を XR-410 のアドレスとしておけば、プロバイダから通知される DNS サーバアドレスが変わったとしても、ホスト側では DNS のアドレスを変えることなく、そのままアクセスできます。

◆DNS キャッシュ機能

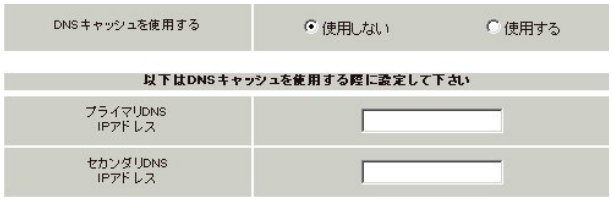
インターネット上のサイトにアクセスするときは、アクセスのたびに DNS サーバへ名前解決を要求しています。

しかし DNS サーバとの通信に時間がかかってしまい、結果的にアクセスが遅くなってしまうということも起こり得ます。

そこで DNS キャッシュ機能を使うことで名前解決の結果を XR-410 が記憶しておき、次回からの名前解決要求時には実際の DNS サーバからの応答を待つのではなく、キャッシュ上に名前解決結果が残っていればそれを使うことで、高速な名前解決が可能になります。

11. DNS キャッシュ機能の設定

Web 設定画面「各種サービスの設定」->「DNS サーバ」をクリックして、以下の画面で設定します。



○ DNS キャッシュ機能の ON/OFF を選択します。
また DNS キャッシュ機能を使う場合は、ISP から指定されたもの、もしくは任意の DNS サーバの IP アドレスを指定してください。

最後に「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

各種サービスの設定画面で DNS サーバを「停止」にすると、XR-410 の DNS リレー機能も停止してしまいます。この場合は各ホスト / サーバに DNS サーバアドレスを設定する必要があります。

第 11 章

DHCP サーバ / リレー機能

第 11 章 DHCP サーバ / リレー機能

Ⅰ．XR-410 の DHCP 関連機能について

XR-410 は、以下の 4 つの DHCP 関連機能を搭載しています。

◆ DHCP クライアント機能

本装置のインターネット /WAN 側ポートは DHCP クライアントとなることができますので、IP アドレスの自動割り当てをおこなう CATV インターネット接続サービスで利用できます。

また既存 LAN に仮設 LAN を接続したい場合などに、XR-410 の IP アドレスを決めなくても既存 LAN から IP アドレスを自動的に取得でき、LAN 同士の接続が容易に可能となります。

DHCP クライアント機能の設定は［第 5 章 インターフェース設定］を参照してください。

◆ DHCP サーバ機能

本装置のインタフェースは DHCP サーバとなることができますので、LAN 側のコンピューターに自動的に IP アドレス等の設定をおこなえます。

◆ IP アドレスの固定割り当て

DHCP サーバ機能では通常、使用されていない IP アドレスを順に割り当てる仕組みになっていますので、DHCP クライアントの IP アドレスは変動することがあります。しかし固定割り当ての設定をすることで、DHCP クライアントの MAC アドレス毎に常に同じ IP アドレスを割り当てることができます。

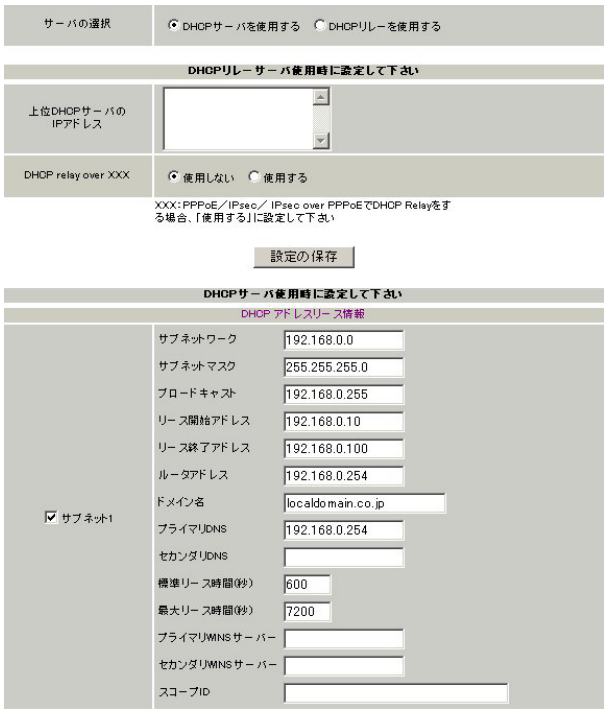
◆ DHCP リレー機能

DHCP サーバと DHCP クライアントは通常、同じネットワークにないと通信できません。しかし XR-410 の DHCP リレー機能を使うことで、異なるネットワークにある DHCP サーバを利用できるようになります(XR-410 が DHCP クライアントからの要求と DHCP サーバからの応答を中継します)。

DHCP リレー機能は NAT 機能を利用している場合の利用はできません。

11. DHCP サーバ機能の設定

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」をクリックして、以下の画面で設定をおこないます。



(実際の画面には「サブネット 2」項目も表示されます)

DHCP サーバ / リレー機能設定

画面上部「DHCP サーバの設定」をクリックします。

○サーバの選択
DHCP サーバ機能 / リレー機能のどちらを使うかを選択します。サーバ機能とリレー機能を同時に使うことはできません。

○上位 DHCP サーバの IP アドレス
DHCP リレー機能を使う場合に、上位の DHCP サーバの IP アドレスを指定してください。

○ DHCP relay over xxx
PPPoE・IPsec・PPPoE 接続時の IPsec 上で DHCP リレー機能を利用する場合に「使用する」に設定して下さい。

○サブネット
DHCP サーバ機能の動作設定をおこないます。
・複数のサブネットを設定することができます。
・どのサブネットを使うかは、XR-410 のインターフェースに設定された IP アドレスを参照の上、同じサブネットとなる設定を使います。
・ラジオボックスにチェックを入れたサブネット設定が、参照・動作の対象となります。

各サブネットごとの詳細設定は以下の通りです。

○サブネットワーク
DHCP サーバ機能を有効にするサブネットワーク空間のアドレスを指定します。

○サブネットマスク
DHCP サーバ機能を有効にするサブネットワーク空間のサブネットマスクを指定します。

○ブロードキャスト
DHCP サーバ機能を有効にするサブネットワーク空間のブロードキャストアドレスを指定します。

○リース開始アドレス / 終了アドレス
DHCP クライアントに割り当てる最初と最後の IP アドレスを指定します(割り当て範囲となります)。

○ルータアドレス
DHCP クライアントのデフォルトゲートウェイとなるアドレスを入力してください。通常は、XR-410 のインタフェースの IP アドレスを指定します。

○ドメイン名
DHCP クライアントに割り当てるドメイン名を入力します。必要であれば指定してください。

○プライマリ / セカンダリ DNS
DHCP クライアントに割り当てる DNS サーバアドレスを指定します。必要であれば指定してください。

(次のページに続きます)

III. DHCP サーバ機能の設定例

○標準リース時間
DHCP クライアントに IP アドレスを割り当てる時間を指定します。単位は秒です。初期設定では 600 秒になっています。

○最大リース時間
DHCP クライアント側が割り当て時間を要求してきたときの、最大限の割り当て時間を指定します。単位は秒です。初期設定では 7200 秒になっています。(7200 秒以上のリース時間要求を受けても、7200 秒がリース時間になります)

○プライマリ / セカンダリ WINS サーバー
DHCP クライアントに割り当てる WINS サーバの IP アドレスを指定します。

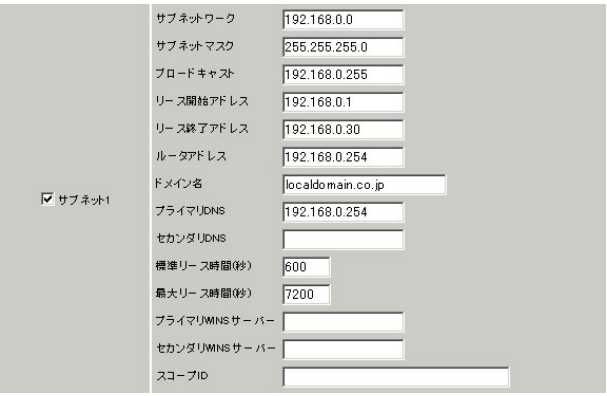
○スコープ ID
NetBIOS スコープ ID を配布できます。
TCP/IP を介して NetBIOS を実行しているコンピュータでは、同じ NetBIOS スコープ ID を使用するほかのコンピュータとのみ NetBIOS 情報を交換することができます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

DHCP サーバ機能の設定例

- LAN は 192.168.0.0/24 のネットワーク
- 192.168.0.1 から 30 のアドレスをリース
- ルータアドレスは 192.168.0.254
- ルータは DNS リレー機能が有効
- 標準リース時間は 1 時間
- 最大リース時間は 5 時間

上記条件の場合の設定例です。

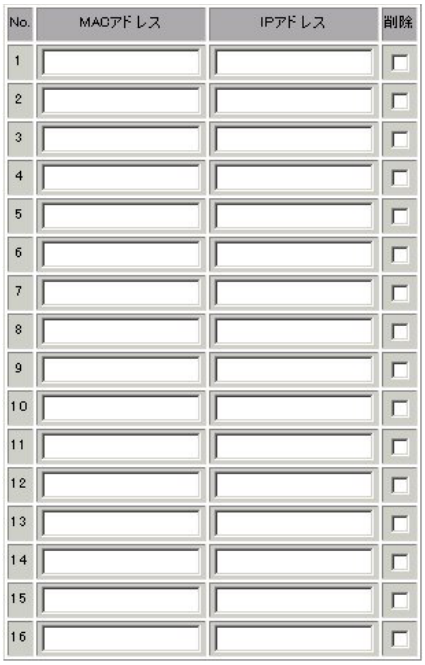


IV. IP アドレス固定割り当て設定

DHCP サーバ機能を利用して、特定のクライアントに特定の IP アドレスを固定で割り当てる場合は、以下の手順で設定します。

設定方法

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」→画面上部の「DHCP IP アドレス固定割り付け設定」をクリックして、以下の画面で設定をおこないます。



○ MAC アドレス
コンピューターに装着されている LAN ボードなどの MAC アドレスを入力します。
＜入力例＞　*00:80:6d:49:ff:ff*

○ IP アドレス
その MAC アドレスに固定で割り当てる IP アドレスを入力します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
固定割り当て機能は、DHCP サーバ機能を再起動してから有効になります。

エントリの削除方法

一覧の「削除」項目にチェックして「設定 / 削除の実行」をクリックすると、そのエントリが削除されます。

第 12 章

IPsec 機能

Ⅰ.XR-410 の IPsec 機能について

◆鍵交換について
IKE を使用しています。IKE フェーズ 1 ではメインモード、アグレッシブモードの両方をサポートしています。フェーズ 2 ではクイックモードをサポートしています。
固定 IP アドレス同士の接続はメインモード、固定 IP アドレスと動的 IP アドレスの接続はアグレッシブモードで設定してください。

◆認証方式について
XR-410 シリーズでは「共通鍵方式」「RSA 公開鍵方式」「X.509」による認証に対応しています。
ただしアグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

◆暗号化アルゴリズム
シングル DES とトリプル DES、AES128bit をサポートしています。暗号化処理は XR-410/TX2 はソフトウェア、XR-410/TX2DES はハードウェア処理で行ないます。

◆ハッシュアルゴリズム
SHA1 と MD-5 を使用しています。

◆認証ヘッダ
XR-410 は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

◆DH 鍵共有アルゴリズムで使用するグループ
group1、group2、group5 をサポートしています。

◆ IPsec 使用時の通信可能対地数
64 拠点まで IPsec 接続が可能です。

◆ IPsec とインターネット接続
IPsec 通信をおこなっている場合でも、その設定以外のネットワークへは、通常通りインターネットアクセスが可能です。

◆ FutureNet XR VPN Client との接続において、NAT トラバーサルに対応しています。

他の機器との接続実績について
2004 年 5 月現在で、以下のルータとの接続を確認しています。

- Futurenet　XR シリーズ
- FutureNet XR VPN Clinet(SSH Sentinel)
- Linux サーバ(FreeS/WAN)

11. IPsec 設定の流れ

◆ PreShared(共通鍵)方式での IPsec 通信

STEP 1　共通鍵の決定

IPsec 通信をおこなうホスト同士の認証と、データの暗号化・復号化で使う共通秘密鍵の生成に必要な鍵を任意で決定します。IPsec 通信をおこなう双方で共通の鍵を使います。半角英数字であればどんな文字列でもかまいません。

STEP 2　共通鍵の交換

決定した共通鍵は、第三者に知られないように十分注意して交換してください。共通鍵が第三者に渡ると、その鍵を利用して不正な IPsec 接続が確立されるおそれがあります。

STEP 3　本装置側の設定

自分側の XR-410 の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するための IKE/ISAKMP ポリシー設定をおこないます。ここで共通鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5　IPsec ポリシー設定

IPsec 通信を行う相手側セグメントの設定をおこないます。このとき、どの IKE 設定を使用するかを指定します。

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

◆ RSA(公開鍵)方式での IPsec 通信

STEP 1　公開鍵・暗号鍵の生成

IPsec 通信をおこなうホスト同士の認証とデータの暗号化に必要な公開鍵と、復号化に必要な秘密鍵を生成します。公開鍵は IPsec の通信相手に渡しておきます。鍵の長さを指定するだけで、自動的に生成されます。

STEP 2　公開鍵の交換

鍵を生成すると、設定画面上では公開鍵が表示されます。この鍵を IPsec 通信をおこなう相手側に通知してください。また同様に、相手側が生成した公開鍵を入手してください。公開鍵は第三者に知られても問題ありません。

STEP 3　本装置側の設定

自分側の XR-410 の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するための IKE/ISAKMP ポリシーの設定をおこないます。ここで公開鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5　IPsec ポリシー設定

IPsec通信をおこなう相手側セグメントの設定をおこないます。このとき、どの IKE 設定を使用するかを指定します。

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

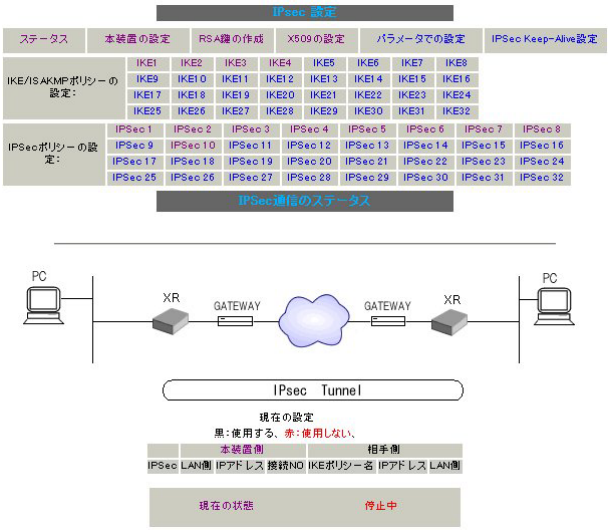
STEP 7　IPsec 接続の確認

IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

III. IPsec 設定

STEP 0　設定画面を開く

Web 設定画面「各種サービスの設定」→「IPsec サーバ」をクリックして、以下の画面から設定します。



- **鍵の作成**
- **本装置の設定**
- **IKE/ISAKAMP ポリシーの設定**
- **IPsec ポリシーの設定**
- **ステータスの確認**
- **パラメータでの設定**

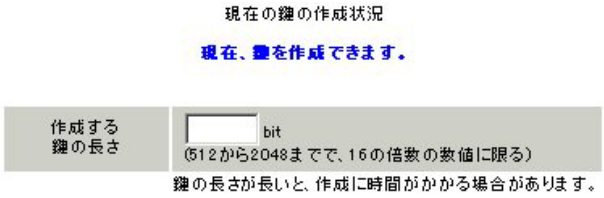
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

STEP 1,2　鍵の作成・交換

RSA 公開鍵方式を用いて IPsec 通信をおこなう場合は、最初に鍵を自動生成します。

PSK 共通鍵方式を用いて IPsec 通信をおこなう場合は、「鍵の作成」は不要です。相手側と任意で共通鍵を決定し、交換しておきます。

1 IPsec 設定画面上部の「RSA 鍵の作成」をクリックして、以下の画面を開きます。



2 作成する鍵の長さを指定して「公開鍵の作成」をクリックします。
鍵の長さは 512bit から 2048bit までで、16 の倍数となる数値が指定可能です。
現在の鍵の作成状況が「鍵を作成できます」の表示の時に限り、作成可能です。

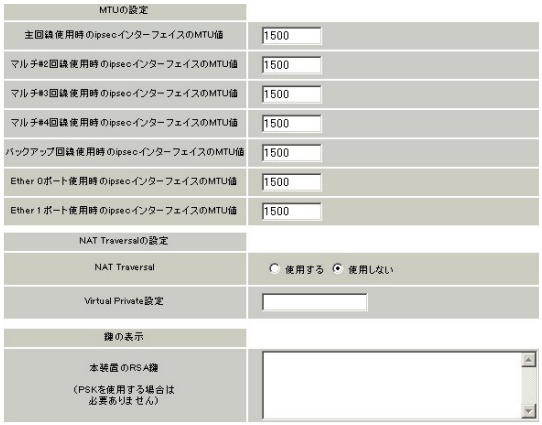
3 鍵を生成します。**「鍵を作成しました。」**のメッセージが表示されると、鍵の生成が完了です。
生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。
またこの鍵は公開鍵となりますので、相手側にも通知してください。

STEP 3　本装置側の設定をおこなう

IPsec 設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]

「本装置の設定」をクリックします。



○ MTU の設定

IPsec 接続時の MTU 値を設定します。
各インタフェースごとに設定できます。
通常は初期設定のままでかまいません。

○ NAT Traversal の設定

NAT トラバーサル機能を使うことで、NAT 環境下にあるクライアントと IPsec 通信を行えるようになります。

「NAT Traversal」
NAT トラバーサル機能を使うかどうかを選択します。

「Virtual Private 設定」
接続相手のクライアントが属しているネットワークと同じネットワークアドレスを入力します。以下のような書式で入力してください。

%v4:<ネットワーク>/<マスクビット値>

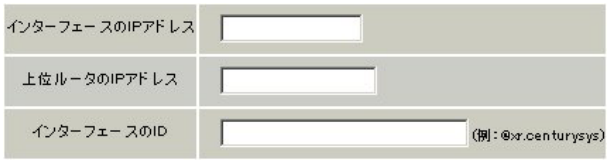
NAT Traversal を使う時のみ設定します。

○鍵の表示

RSA 鍵の作成をおこなった場合ここに、作成した本装置の RSA 公開鍵が表示されます。
PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

[本装置側の設定]

「本装置側の設定」の 1～8 のいずれかをクリックします。ここで XR-410 自身の IP アドレスやインタフェース ID を設定します。



○インターフェースの IP アドレス

[固定アドレスの場合]
本装置に設定されている IP アドレスをそのまま入力します。

[動的アドレスの場合]
PPP/PPPoE 主回線接続の場合は「%ppp0」と入力します。Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1)」と入力します。

○上位ルータの IP アドレス

本装置から見て 1 つ上位のルータ(ゲートウェイ)の IP アドレスを入力します。

[固定アドレスの場合]
上位ルータの IP アドレスをそのまま入力します。**PPP/PPPoE 接続の場合は「%ppp0」と入力してください。**

[動的アドレスの場合]
空欄のままにします。

○インターフェースの ID

本装置への IP アドレスの割り当てが動的割り当ての場合(agressive モードで接続する場合)は、インタフェースの ID を設定します（必須)。

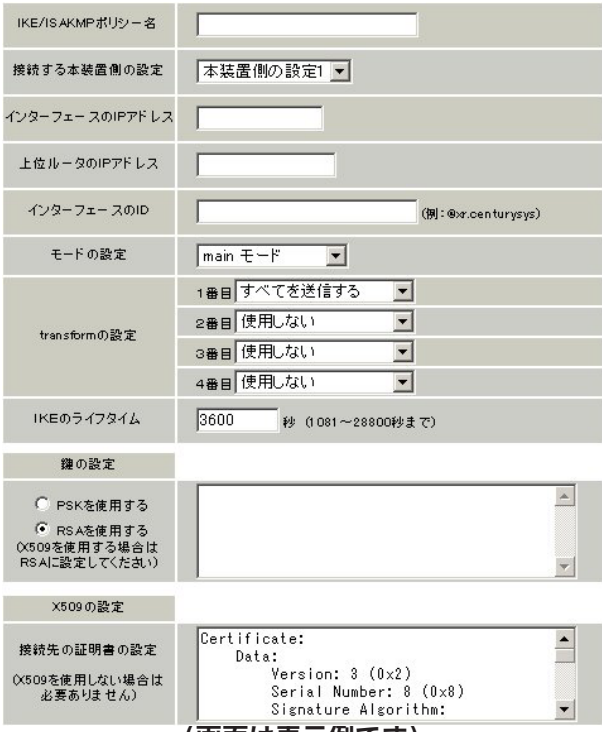
<入力形式>　**@<任意の文字列>**
<入力例>　@centurysystems

@ の後は、任意の文字列でかまいません。

最後に「設定の保存」をクリックして設定完了です。続いて **IKE/ISAKMAP ポリシー**の設定をおこないます。

STEP 4　IKE/ISAKMAP ポリシーの設定

IPsec 設定画面上部の「IKE/ISAKAMP ポリシーの設定」1～32 のいずれかをクリックして、以下の画面から設定します。



(画面は表示例です)

32 個以上の IKE/ISAKMP ポリシーを設定する場合は、画面上部の「パラメータの設定」をクリックして、パラメータでの設定を行なってください。

○ IKE/ISAKAMP ポリシー名

設定名を任意で設定します。(省略可)

○インターフェースの IP アドレス

相手側 IPsec 装置の IP アドレスを設定します。相手側装置への IP アドレスの割り当てが固定か動的かで、入力が異なります。

[**相手側装置が固定アドレスの場合**]

IP アドレスをそのまま入力します。

[**相手側装置が動的アドレスの場合**]

「0.0.0.0」を入力します。

○上位ルータの IP アドレス

相手側装置から見て 1 つ上位のルータ(主にゲートウェイ)IP アドレスを入力します。

本装置への IP アドレスの割り当てが固定か動的かで、入力が異なります。

[**相手側装置が固定アドレスの場合**]

上位ルータの IP アドレスをそのまま入力します。

<u>相手側装置が PPP、PPPoE 接続の場合は、空欄にしておきます。</u>

[**相手側装置が動的アドレスの場合**]

空欄のままにします。

○インタフェースの ID

対向側装置への IP アドレスの割り当てが動的割り当ての場合に限り、IP アドレスの代わりに ID を設定します。

<入力形式>　**@<任意の文字列>**

<入力例>　@centurysystems

@の後は、任意の文字列でかまいません。

<u>対向側装置への割り当てが固定アドレスの場合は設定の必要はありません。</u>

○モードの設定

IKE のフェーズ 1 モードを「main モード」と「agressive モード」のどちらかから選択します。

(次ページに続きます)

III. IPsec 設定

○ transform の選択
ISAKMP SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。XR-410 は、以下のものの組み合わせが選択できます。

- DH group 値　　(group1、group2、group5)
- 暗号化アルゴリズム (des、3des、aes)
- 認証アルゴリズム　(md5、sha1)

「agressive モード」の場合、接続相手の機器に合わせて transform を選択する必要があります。agressive モードでは transform を 1 つだけ選択してください(2 番目～4 番目は「使用しない」を選択しておきます)。

「main モード」の場合も transform を選択できますが、基本的には「すべてを送信する」の設定で構いません。

○ IKE のライフタイム
ISAKMP SA のライフタイムを設定します。ISAKMP SA のライフタイムとは、双方のホスト認証と秘密鍵を交換するトンネルの有効期間のことです。
1081 ～ 28800 秒の間で設定します。

○鍵の設定
[PSK 方式の場合]
「PSK を使用する」にチェックして、相手側と任意に決定した共通鍵を入力してください。

[RSA 公開鍵方式の場合]
「RSA を使用する」にチェックして、相手側から通知された公開鍵を入力してください。「X.509」設定の場合も「RSA を使用する」にチェックします。

○ X509 の設定
「X.509」設定で IPsec 通信をおこなう場合は、相手側装置に対して発行されたデジタル証明書をテキストボックス内に貼り付けます。

最後に「設定の保存」をクリックして設定完了です。

続いて、IPsec ポリシーの設定をおこないます。

III. IPsec 設定

STEP 5　IPsec ポリシーの設定

IPsec 設定画面上部の「IPsec ポリシーの設定」をクリックして、以下の画面から設定します。

(画面は表示例です)

32 個以上の IPsec ポリシーを設定する場合は、画面上部の「パラメータの設定」をクリックして、パラメータでの設定を行なってください。

○最初に IPsec の起動状態を選択します。
「使用する」は initiater にも responder にもなります。
「使用しない」は、その IPsec ポリシーを使用しません。
「Responder として使用する」は XR-410 が固定 IP アドレス設定で接続相手が動的 IP アドレス設定の場合に選択します。
「On-Demand で使用する」は、IPsec をオンデマンド接続します。切断タイマーは SA のライフタイムとなります。

○使用する IKE ポリシー名の選択
STEP 4 で設定した IKE/ISAKMP ポリシーのうち、どのポリシーを使うかを選択します。

○本装置側の LAN 側のネットワークアドレス
自分側の XR-410 に接続している LAN のネットワークアドレスを入力します。ネットワークアドレス / マスクビット値の形式で入力します。
[入力例]　***192.168.0.0/24***

○相手側の LAN 側のネットワークアドレス
相手側の IPsec 装置に接続されている LAN のネットワークアドレスを入力します。ネットワークアドレス / マスクビット値の形式で入力します。

また NAT Traversal 機能を使用している場合に限っては、" ***vhost:%priv*** " と設定します。

○ PH2 の TransForm の選択
IPsec SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。

- 暗号化アルゴリズム　(des、3des、aes)
- 認証アルゴリズム　(md5、sha1)

通常は「すべてを送信する」の選択で構いません。

○ PFS
PFS(PerfectForwardSecrecy)を「使用する」か「使用しない」かを選択します。
PFS とは、パケットを暗号化している秘密鍵が解読されても、その鍵ではその後に生成された鍵を解読できないようにするものです。装置への負荷が増加しますが、より高いセキュリティを保つためには PFS を使用することを推奨します。

○ DH Group の選択(PFS 使用時に有効)
「PFS を使用する」場合に使用する DH group を選択します。ただし「指定しない」を選択しても構いません。その場合は、すべての DH Group 条件を接続相手に送ります。

○ SA のライフタイム
IPsec SA の有効期間を設定します。IPsecSA とはデータを暗号化して通信するためのトラフィックのことです。1081 ～ 86400 秒の間で設定します。

○ DISTANCE
IPsec ルートのディスタンス値を設定できます。
IPsec ルートを OSPF で再配信する場合は、「OSPF 機能設定」の「static ルートの再配信」を「有効」にする必要があります。

III. IPsec 設定

最後に「設定の保存」をクリックして設定完了です。続いて、IPsec 機能の起動をおこないます。

[IPsec 通信時の Ethernet ポート設定について]
IPsec 設定をおこなう場合は、Ethernet ポートの設定に注意してください。

IPsec通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-410 の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 の設定で、且つ、XR-410 の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

このような場合は XR-410 の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

STEP 6　IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

○動作状態の制御
IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、XR-410 を起動するたびに IPsec 機能が自動起動します。
IPsec 機能を止める場合は「停止」にチェックして「動作変更」をクリックしてください。

IPsec 機能を起動した後は、現在のサービス稼働状況が「動作中」と表示されます。

起動する IKE/ISAKMP ポリシー、IPsec ポリシーが増えるほど、IPsec の起動に時間がかかります。起動が完了するまで数十分かかる場合もあります。

III. IPsec 設定

STEP 7　IPsec 接続を確認する

IPsec が正常に接続したかどうかは、「システム設定」の「ログの表示」でログを確認します。

ログの中で、以下のメッセージが含まれているかを確認してください（ログメッセージは「メインモード」で通信した場合の表示例です）。

Aug　1 12:00:20 localhost ipsec__plutorun: 004 "xripsec1" #1: **STATE_MAIN_I4: ISAKMP SA established　・・・(1)**

及び

Aug　1 12:00:20 localhost ipsec__plutorun: 004 "xripsec1" #2: **STATE_QUICK_I2: sent QI2, IPsec SA established　・・・(2)**

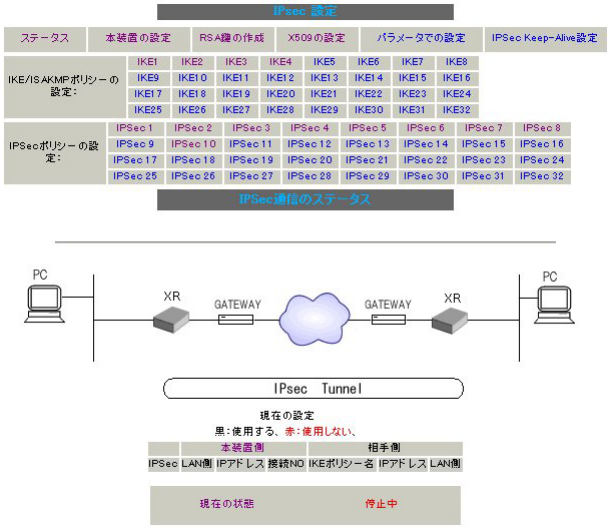
上記 2 つのメッセージが表示されていれば、IPsec が正常に接続されています。

(1)のメッセージは、IKE 鍵交換が正常に完了し、ISAKMP SA が確立したことを示しています。

(2)のメッセージは、IPsec SA が正常に確立したことを示しています。

STEP 8　IPsec ステータス確認の確認

IPsec の簡単なステータスを確認できます。
「各種サービスの設定」→「IPsec サーバ」→「ステータス」をクリックして、画面を開きます。



それぞれの対向側設定でおこなった内容から、本装置・相手側の LAN アドレス・IP アドレス・上位ルータアドレスの一覧や、現在の動作状況が表示されます。

「現在の状態」リンクをクリックすると、現在の IPsec の状況が表示されます。

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

IV. IPsec Keep-Alive 機能

IPsec Keep-Alive 機能は、IPsec トンネルの障害を検出する機能です。

指定した宛先へ IPsec トンネル経由で ping パケットを発行して応答がない場合に IPsec トンネルに障害が発生したと判断し、その IPsec トンネルを自動的に削除します。不要な IPsec トンネルを自動的に削除することで、IPsec の再接続性を高めます。

IPsec 設定画面上部の「IPsecKeep-Alive 設定」をクリックして設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	delay(sec)	flag	interface	slave SA	remove?
1	☐			30	6	180	☐	ipsec0		☐
2	☐			30	6	180	☐	ipsec0		☐
3	☐			30	6	180	☐	ipsec0		☐
4	☐			30	6	180	☐	ipsec0		☐
5	☐			30	6	180	☐	ipsec0		☐
6	☐			30	6	180	☐	ipsec0		☐
7	☐			30	6	180	☐	ipsec0		☐
8	☐			30	6	180	☐	ipsec0		☐
9	☐			30	6	180	☐	ipsec0		☐
10	☐			30	6	180	☐	ipsec0		☐
11	☐			30	6	180	☐	ipsec0		☐
12	☐			30	6	180	☐	ipsec0		☐
13	☐			30	6	180	☐	ipsec0		☐
14	☐			30	6	180	☐	ipsec0		☐
15	☐			30	6	180	☐	ipsec0		☐
16	☐			30	6	180	☐	ipsec0		☐

○ enable
設定を有効にする時にチェックします。IPsec Keep-Alive 機能を使いたい IPsec ポリシーと同じ番号にチェックを入れます。

○ source address
IPsec 通信を行う際の、XR の LAN 側インターフェースの IP アドレスを入力します。

○ destination address
IPsec 通信を行う際の、XR の対向側装置の LAN 側のインターフェースの IP アドレスを入力します。

○ interval(sec)
○ watch count
ping を発行する間隔を設定します。
「『interval(sec)』間に『watch count』回 ping を発行する」という設定になります。

○ delay(sec)
IPsec が起動してから ping を発行するまでの待ち時間を設定します。IPsec が確立するまでの時間を考慮して設定します。

○ flag
チェックを入れると、delay 後に ping を発行して、ping が失敗したら即座に指定された IPsec トンネルの削除、再折衝を開始します。また Keep-Alive によって SA 削除後は、毎回 delay 時間待ってから Keep-Alive が開始されます。
チェックはずすと、delay 後に最初に ping が成功(IPsec が確立)し、その後に ping が失敗してはじめて指定された IPsec トンネルの削除、再折衝を開始します。IPsec が最初に確立する前に ping が失敗してもなにもしません。また delay は初回のみ発生します。

○インタフェース
Keep-Alive 機能を使う、本装置の IPsec インタフェース名を入力します。

○ backup SA
ここに IPsec ポリシーの設定番号を指定しておくと、IPsec Keepalaive 機能で IPsec トンネルを削除した時に、ここで指定したポリシー設定を起動させます。1 つの設定番号のみ指定可能です。

○ remove
設定を削除したいときにチェックします。

最後に「設定 / 削除の実行」をクリックしてください。remove 項目にチェックが入っているものについては、その設定が削除されます。

設定番号について
IPsec Keep-Alive 機能を使う際は、監視する IPsec のポリシー No. と Keepalive の No. は一致させてください。

IPsec トンネルの障害を検知する条件
IPsec Keep-Alive 機能によって障害を検知するのは、「interval/watch count」に従って ping を発行して、一度も応答がなかったときです。
このとき本装置は、ping の応答がなかった IPsec トンネルを自動的に削除します。
反対に一度でも応答があったときは、本装置は IPsec トンネルを保持します。

V.「X.509 デジタル証明書」を用いた電子認証

XR-410 は X.509 デジタル証明書を用いた電子認証方式に対応しています。

ただし XR-410 は証明書署名要求の発行や証明書の発行ができませんので、あらかじめ CA 局から証明書の発行を受けておく必要があります。

電子証明の仕組みや証明書発行の詳しい手順につきましては関連書籍等をご参考下さい。

情報処理振興事業協会セキュリティセンター
http://www.ipa.go.jp/security/pki/

設定は、IPsec 設定画面内の「X.509 の設定」から行えます。

[X.509 の設定]
「X.509 の設定」画面→「X.509 の設定」を開きます。

○ X509 の設定
X.509 の使用 / 不使用を選択します。

○証明書のパスワード
証明書のパスワードを入力します。

V.「X.509 デジタル証明書」を用いた電子認証

[CA の設定]
ここには、CA 局自身のデジタル証明書の内容をコピーして貼り付けます。

[本装置側の証明書の設定]
ここには、本装置に対して発行されたデジタル証明書の内容をコピーして貼り付けます。

[本装置側の鍵の設定]
ここにはデジタル証明書と同時に発行された、本装置の秘密鍵の内容をコピーして貼り付けます。

[失効リストの設定]
失効リストを作成している場合は、その内容をコピーして貼り付けます。

[その他の設定について]
その他の設定については、通常の IPsec 設定と同様にしてください。

その際、「IKE/ISAKMAP ポリシーの設定」画面内の鍵の設定項目は、「RSA を使用する」にチェックします。鍵は空欄のままにします(「本装置の設定」画面の鍵表示も空欄のままです)。

以上で X.509 の設定は完了です。

[設定のバックアップ保存について]
設定のバックアップを作成しても、X.509 関連の設定は含まれません。またパラメータによる設定にも反映されません。

バックアップファイルから設定を復帰させる場合でも、X.509 関連の設定は再度おこなってください。

VI. IPsec 通信時のパケットフィルタ設定

ステートフルパケットインスペクション機能を使っていたり、パケットフィルタの設定によっては、IPsec 通信ができない場合があります。
このような場合は IPsec 通信でのデータをやりとりできるように、パケットフィルタの設定を追加する必要があります。

IPsec では、以下の 2 種類のプロトコル・ポートを使用します。

- **プロトコル「UDP」のポート「500」番**
  ->IKE(IPsec の鍵交換)のトラフィックに必要です

- **プロトコル「ESP」**
  ->ESP(暗号化ペイロード)のトラフィックに必要です

これらのパケットを通せるように、**「入力フィルタ」**に設定を追加してください。なお、「ESP」については、ポート番号の指定はしません。

< 設定例 >

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1	パケット受信時	許可	udp				500
PPP/PPPoE－主回線 #1	パケット受信時	許可	esp				

VII. IPsec がつながらないとき

IPsec で正常に通信できないときは本体ログを確認することで、どの段階で接続に失敗しているかを把握することができます。

本体ログは、「システム設定」内の「ログ表示」で確認します。

[正常に IPsec 接続できたときのログメッセージ]

メインモードの場合

```
Aug  3 12:00:14 localhost ipsec_setup:
 ...FreeS/WAN IPsec started

Aug  3 12:00:20 localhost ipsec__plutorun:
 104 "xripsec1" #1: STATE_MAIN_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 106 "xripsec1" #1: STATE_MAIN_I2: from
 STATE_MAIN_I1; sent MI2, expecting MR2

Aug  3 12:00:20 localhost ipsec__plutorun:
 108 "xripsec1" #1: STATE_MAIN_I3: from
 STATE_MAIN_I2; sent MI3, expecting MR3

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
 established

Aug  3 12:00:20 localhost ipsec__plutorun:
 112 "xripsec1" #2: STATE_QUICK_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #2: STATE_QUICK_I2: sent QI2,
 IPsec SA established
```

アグレッシブモードの場合

```
Apr 25 11:14:27 localhost ipsec_setup:
...FreeS/WAN IPsec started

Aug 3 11:14:34 localhost ipsec__plutorun: whack:
ph1_mode=aggressive whack:CD_ID=@home
whack:ID_FQDN=@home 112 "xripsec1" #1:
STATE_AGGR_I1: initiate

Aug 3 11:14:34 localhost ipsec__plutorun: 004
"xripsec1" #1: SAEST(e)=STATE_AGGR_I2: sent AI2,
ISAKMP SA established

Aug 3 12:14:34 localhost ipsec__plutorun: 117
"xripsec1" #2: STATE_QUICK_I1: initiate

Aug 3 12:14:34 localhost ipsec__plutorun: 004
"xripsec1" #2: SAEST(13)=STATE_QUICK_I2: sent QI2,
IPsec SA established
```

VII. IPsec がつながらないとき

「現在の状態」は IPsec 設定画面の「ステータス」から、画面中央下の「現在の状態」をクリックして表示します。

[正常に IPsec が確立したときの表示例]

```
000 interface ipsec0/eth1 218.xxx.xxx.xxx

000

000 "xripsec1": 192.168.xxx.xxx/24
===218.xxx.xxx.xxx[@<id>]---218.xxx.xxx.xxx...

000 "xripsec1": ...219.xxx.xxx.xxx
===192.168.xxx.xxx.xxx/24

000 "xripsec1":   ike_life: 3600s; ipsec_life:
28800s; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0

000 "xripsec1":   policy: PSK+ENCRYPT+TUNNEL+PFS;
interface: eth1; erouted

000 "xripsec1":   newest ISAKMP SA: #1; newest
IPsec SA: #2; eroute owner: #2

000

000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec
SA established); EVENT_SA_REPLACE in 27931s;
newest IPSEC; eroute owner

000 #2: "xripsec1" esp.32a406c4@219.xxx.xxx.xxx
esp.1be9611c@218.xxx.xxx.xxx
tun.1002@219.xxx.xxx.xxx tun.1001@218.xxx.xxx.xxx

000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA
established); EVENT_SA_REPLACE in 2489s; newest
ISAKMP
```

これらのログやメッセージ内に

- **ISAKMP SA established**
- **IPsec SA established**

のメッセージがない場合は IPsec が確立していません。設定を再確認して下さい。

VII. IPsec がつながらないとき

○「 ...FreeS/WAN IPsec started」でメッセージが止まっています。

この場合は、接続相手との IKE 鍵交換が正常に行えていません。
IPsec 設定の「IKE/ISAKMP ポリシーの設定」項目で相手側機器についての設定を確認してください。

また、ステートフルパケットインスペクションを有効にしている場合、IPsec 通信のパケットを受信できるようにフィルタ設定を施す必要があります。IPsec のパケットを通すフィルタ設定は、「VI. IPsec 通信時のパケットフィルタ設定」をご覧ください。

○「ISAKMP SA established」メッセージは表示されていますが「IPsec SA established」メッセージが表示されていません。

この場合は、IPsec SA が正常に確立できていません。
IPsec 設定の「IPsec ポリシー設定」項目で、自分側と相手側のネットワークアドレスが正しいか、設定を確認してください。

○新規に設定を追加したのですが、追加した設定については IPsec がつながりません。

設定を追加し、その設定を有効にする場合には IPsec 機能を再起動(本体の再起動)を行ってください。設定を追加しただけでは設定が有効になりません。

○ IPSec は確立していますが、Windows でファイル共有ができません。

XR シリーズは工場出荷設定において、NetBIOS を通さないフィルタリングが設定されています。Windows ファイル共有をする場合はこのフィルタ設定を削除もしくは変更してください。

○ aggressive モードで接続しようとしたら、今までつながっていた IPsec がつながらなくなってしまいました。

固定 IP - 動的 IP 間での main モード接続と aggressive モード接続を共存させることはできません。

このようなトラブルを避けるために、固定 IP - 動的 IP 間で IPsec 接続する場合は aggressive モードで接続するようにしてください。

○ IPsec 通信中に回線が一時的に切断してしまうと、回線が回復しても IPsec 接続がなかなか復帰しません。

固定 IP アドレスと動的 IP アドレス間の IPsec 通信で、固定 IP アドレス側装置の IPsec 通信が意図しない切断をしてしまったときに起こりえる現象です。

相手が動的 IP アドレスの場合は相手側の IP アドレスが分からないために、固定 IP アドレス側からは IPsec 通信を開始することが出来ず、動的 IP アドレス側から IPsec 通信の再要求を受けるまでは IPsec 通信が復帰しなくなります。また動的側 IP アドレス側が IPsec 通信の再要求を出すのは IPsec SA のライフタイムが過ぎてからとなります。

これらの理由によって、IPsec 通信がなかなか復帰しない現象となります。

すぐに IPsec 通信を復帰させたいときは、動的 IP アドレス側の IPsec サービスも再起動する必要があります。

また、「**IPsec Keep-Alive 機能**」を使うことで IPsec の再接続性を高めることができます。

○相手の XR-410 には IPsec のログが出ているのに、こちらの XR-410 にはログが出ていません。IPsec は確立しているようなのですが、確認方法はありませんか？

固定 IP - 動的 IP 間での IPsec 接続をおこなう場合、固定 IP 側(受信者側)の XR-410 ではログが表示されないことがあります。その場合は「各種サービスの設定」→「IPsec サーバ」→「ステータス」を開き、「現在の状態」をクリックして下さい。ここに現在の IPsec の状況が表示されます。

第 13 章

UPnP 機能

第 13 章 UPnP 機能

Ⅰ.UPnP 機能の設定

XR-410 は UPnP(Universal Plug and Play)に対応していますので、UPnP に対応したアプリケーションを使うことができます。

対応している Windows OS とアプリケーション

Windows OS

- Windows XP
- Windows Me

アプリケーション（2004 年 5 月現在）

- Windows Messenger

利用できる Messenger の機能について

以下の機能について動作を確認しています(2004 年 5 月現在)。

- インスタントメッセージ
- 音声チャット
- ビデオチャット
- リモートアクセス
- ホワイトボード

「ファイルまたは写真の送受信」および「アプリケーションの共有」については現在使用できません。

Windows OS の UPnP サービス

Windows XP/Windows Me で UPnP 機能を使う場合は、オプションネットワークコンポーネントとして、ユニバーサルプラグアンドプレイサービスがインストールされている必要があります。UPnP サービスのインストール方法の詳細については Windows のマニュアル、ヘルプ等をご参照ください。

◆UPnP 機能の設定

XR-410 の UPnP 機能の設定は以下の手順でおこなってください。

Web 設定画面「各種サービスの設定」→「UPnP サービス」をクリックして設定します。

○WAN 側インタフェース

WAN 側に接続しているインタフェースを選択します。「主回線」は PPP/PPPoE で接続しているときのインタフェースです。「その他」を選択して、インタフェース名を直接指定もできます。

○LAN 側インタフェース

LAN 側に接続しているインタフェースを選択します。「その他」を選択して、インタフェース名を直接指定もできます。

○切断検知タイマー

UPnP 機能使用時の無通信切断タイマーを設定します。ここで設定した時間だけ無通信時間が経過すると、XR-410 が保持する Windows Messenger のセッションが強制終了されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

第 13 章 UPnP 機能

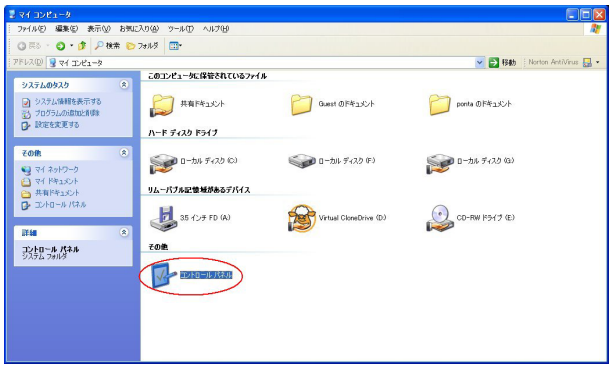
Ⅰ.UPnP 機能の設定

◆UPnP の接続状態の確認

各コンピューターが XR-410 と正常に UPnP で接続されているかどうかを確認します。

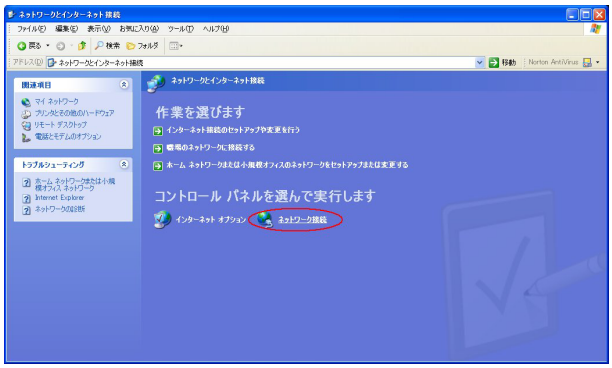
1 「スタート」→「マイコンピュータ」を開きます。

2 「コントロールパネル」を開きます。

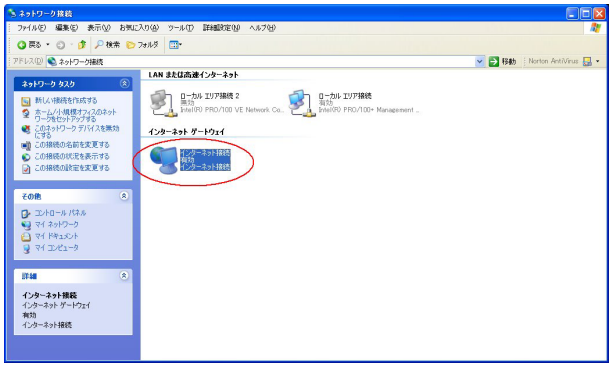


3 「ネットワークとインターネット接続」を開きます。

4 「ネットワーク接続」を開きます。



5 「ネットワーク接続」画面内に、「インターネットゲートウェイ」として**「インターネット接続 有効」**と表示されていれば、正常に UPnP 接続できています。



(画面は Windows XP での表示例です)

Windows OS や Windows Messenger の詳細につきましては、Windows のマニュアル / ヘルプをご参照ください。
弊社では Windows や各アプリケーションの操作法や仕様等についてはお答えできかねますので、ご了承ください。

11.UPnP とパケットフィルタ設定

◆UPnP 機能使用時の注意

UPnP 機能を使用するときは原則として、**WAN 側インタフェースでの「ステートフルパケットインスペクション機能」を無効にしてください。**

ステートフルパケットインスペクション機能を有効にしている場合は、ご利用になる UPnP アプリケーション側で使用する特定のポートをフィルタ設定で開放してください。

参考：NTT 東日本の VoIP-TA の利用ポートは
UDP・5060、UDP・5090、UDP・5091 です。
(詳細は NTT 東日本にお問い合せ下さい)

各 UPnP アプリケーションが使用するポートにつきましては、アプリケーション提供事業者さまにお問い合わせください。

◆UPnP 機能使用時の推奨フィルタ設定

Microsoft Windows 上の UPnP サービスのバッファオーバフロ ーを狙った DoS(サービス妨害)攻撃からの危険性を緩和する為の措置として、XR-410 は工場出荷設定で以下のようなフィルタをあらかじめ設定しています。

(入力フィルタ)

(転送フィルタ)

UPnP 使用時は特に、上記フィルタ設定を作動させておくことを推奨いたします。

第 14 章

ダイナミックルーティング
(RIP と OSPF の設定)

第 14 章 ダイナミックルーティング

Ⅰ．ダイナミックルーティング機能

XR-410 シリーズのダイナミックルーティング機能は、RIP および OSPF をサポートしています。

RIP 機能のみで運用することはもちろん、RIP で学習した経路情報を OSPF で配布することなどもできます。

◆設定の開始

1 Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング」をクリックします。

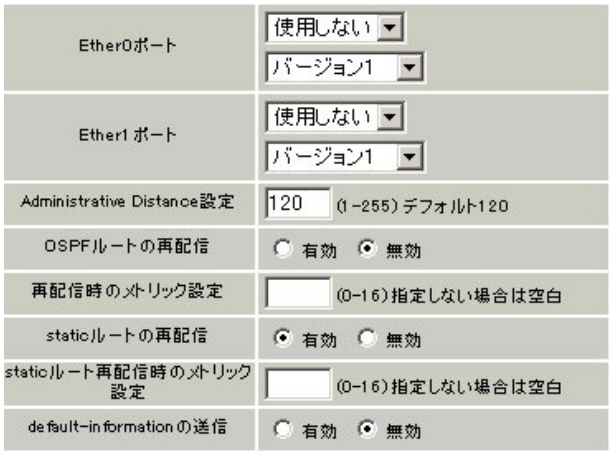
RIP	◉ 停止 ○ 起動	停止中
OSPF	◉ 停止 ○ 起動	停止中

2 「RIP」、「OSPF」をクリックして、それぞれの機能の設定画面を開いて設定をおこないます。

11. RIP の設定

◆RIP の設定

Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング設定」→「RIP」をクリックして、以下の画面から設定します。



○Ether0、Ether1 ポート
XR-410 の各 Ethernet ポートで、RIP の使用 / 不使用、また使用する場合の RIP バージョンを選択します。

○Administrative Distance 設定
RIP と OSPF を併用していて全く同じ経路を学習する場合がありますが、その際はこの値の小さい方を経路として採用します。

○OSPF ルートの再配信
RIP と OSPF を併用していて、OSPF で学習したルーティング情報を RIP で配信したいときに「有効」にしてください。RIP のみを使う場合は「無効」にします。

○再配信時のメトリック設定
OSPF ルートを RIP で配信するときのメトリック値を設定します。

○static ルートの再配信
static ルーティング情報も RIP で配信したいときに「有効」にしてください。RIP のみを使う場合は「無効」にします。

○再配信時のメトリック設定
static ルートを RIP で配信するときのメトリック値を設定します。

○default-information の送信
デフォルトルート情報を RIP で配信したいときに「有効」にしてください。
選択、入力後は「設定」をクリックして設定完了です。

設定後は「ダイナミックルーティング設定」画面に戻り、「起動」を選択して「動作変更」をクリックしてください。

また設定を変更した場合には、「再起動」をクリックしてください。

なお、RIP の動作状況およびルーティング情報は、「RIP 情報の表示」をクリックすることで確認できます。

11. RIP の設定

◆RIP フィルターの設定

RIP による route 情報の送信または受信をしたくないときに設定します。

Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング設定」→「RIP フィルタ設定」をクリックして、以下の画面から設定します。

○NO.
設定番号を指定します。1～64 の間で指定します。

○インタフェース
RIP フィルタを実行するインタフェースを選択します。

○方向
「in-coming」は本装置が RIP 情報を受信する際に RIP フィルタリングします(受信しない)。
「out-going」は本装置から RIP 情報を送信する際に RIP フィルタリングします(送信しない)。

○ネットワーク
RIP フィルタリングの対象となるネットワークアドレスを指定します。

<入力形式>
ネットワークアドレス/サブネットマスク値

入力後は「保存」をクリックしてください。
「取消」をクリックすると、入力内容がクリアされます。

RIP フィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

NO.	インタフェース	方向	ネットワーク	編集 削除
1	Ether0ポート	in-comming	192.168.100.0/24	編集 削除
2	Ether1 ポート	out-going	192.168.0.0/24	編集 削除

「削除」をクリックすると、設定が削除されます。
「編集」をクリックすると、その設定について内容を編集できます。

III．OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

OSPFでは各ルータがリンクステートを交換しあい、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

またOSPFは主に帯域幅からコストを求め、コストがもっとも低いものを最適な経路として採用します。
これにより、トラフィックのロードバランシングが可能となっています。

その他、ホップ数に制限がない、リンクステートの更新にIPマルチキャストを利用する、RIPより収束が早いなど、大規模なネットワークでの利用に向いています。

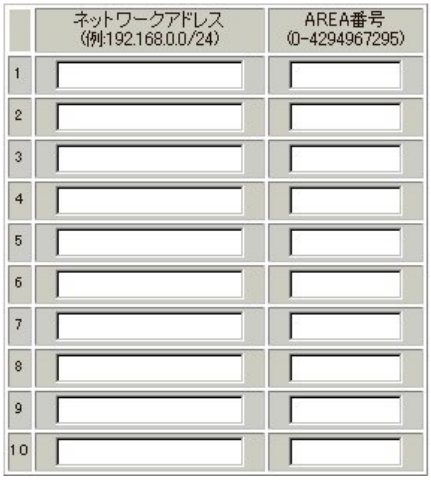
OSPFの具体的な設定方法に関しましては、弊社サポートデスクでは対応しておりません。
専門のコンサルティング部門にて対応いたしますので、その際は弊社までご連絡ください。

OSPF設定は、Web設定画面「各種サービスの設定」→画面左「ダイナミックルーティング設定」→「OSPF」をクリックします。

◆インタフェースへのOSPFエリア設定

どのインタフェースでOSPF機能を動作させるかを設定します。

設定画面上部の「インタフェースへのOSPFエリア設定」をクリックします。



○ネットワークアドレス
XR-410に接続しているネットワークのネットワークアドレスを指定します。**ネットワークアドレス/マスクビット値**の形式で入力します。

○AREA番号
そのネットワークのエリア番号を指定します。

※AREA：リンクステートアップデートを送信する範囲を制限するための論理的な範囲

入力後は「設定」をクリックして設定完了です。

III. OSPF の設定

◆ OSPF エリア設定

各AREA(エリア)ごとの機能設定をおこないます。

設定画面上部の「OSPF エリア設定」をクリックします。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

○ AREA 番号
機能設定をおこなうエリアの番号を指定します。

○スタブ設定
外部に通じる経路がひとつしかない場合や最適な経路を通る必要がない場合にはスタブエリアに指定します。スタブエリアに指定するときは「有効」を選択します。スタブエリアには LSA type5 を送信しません。

○トータリースタブ設定
LSA type5 に加え、type3、4 も送信しないエリアに指定するときに「有効」にします。

○ default-cost 設定
スタブエリアに対してデフォルトルート情報を送信する際のコスト値をしていします。指定しない場合は 1 です。

○認証設定
該当エリアでパスワード認証か MD5 認証をおこなうかどうかを選択します。デフォルト設定は「使用しない」です。

○エリア間ルートの経路集約設定
経路情報を集約して送信したいときに設定します。
Ex: 128.213.64.0 ～ 128.213.95.0 のレンジのサブネットを渡すときに 1 つずつ渡すのではなく、128.213.64.0/27 に集約して渡す、といったときに使用します。ただし、連続したサブネットでなければなりません(レンジ内に存在しないサブネットがあってはなりません)。

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。

	AREA番号	STUB	Totally STUB	Default-cost	Authentication	経路集約	Configure
1	1	有効	無効	10	無効	192.168.10.1 /29	Edit,Remove

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。(画面は表示例です)

III. OSPF の設定

◆OSPF VirtualLink 設定

OSPF において、すべてのエリアはバックボーンエリア(エリア 0)に接続している必要があります。もし接続していなければ、他のエリアの経路情報は伝達されません。

しかし物理的にバックボーンエリアに接続できない場合には VirtualLink を設定して、論理的にバックボーンエリアに接続させます。

設定画面上部の「VirtualLink 設定」をクリックして設定します。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

○ Transit AREA 番号
VirtualLink を設定する際に、バックボーンと設定するルータのエリアが接続している共通のエリアの番号を指定します。このエリアが「Transit AREA」となります。

○ Remote-ABR Router-ID 設定
VirtualLink を設定する際のバックボーン側のルータ ID を設定します。

○ Hello インターバル設定
Hello パケットの送出間隔を設定します。

○ Dead インターバル設定
Dead タイムを設定します。

○ Retransmit インターバル設定
LSA を送出する間隔を設定します。

○ transmit delay 設定
LSU を送出する際の遅延間隔(delay)を設定します。

○認証パスワード設定
VirtualLink 上で simple パスワード認証を使用する際のパスワードを設定します。

○ MD5 KEY-ID 設定(1)
MD5 認証使用時の KEY ID を設定します。

○ MD5 パスワード設定(1)
エリア内で MD5 認証を使用する際の MD5 パスワードを設定します。

○ MD5 KEY-ID 設定(2)
○ MD5 パスワード設定(2)
MD5 KEY-ID とパスワードは 2 つ同時に設定可能です。その場合は(2)に設定します。

VirtualLink 設定では、スタブエリアおよびバックボーンエリアを Transit AREA として設定することはできません。

入力後は「設定」をクリックしてください。

設定後は「VirtualLink 設定」画面に、設定内容が一覧で表示されます。

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。

III. OSPF の設定

◆ OSPF 機能設定

OSPF の動作について設定します。設定画面上部の「OSPF 機能設定」をクリックして設定します。

○ Router-ID 設定

neighbor を確立した際に、ルータの ID として使用されたり、DR、BDR の選定の際にも使用されます。指定しない場合は、ルータが持っている IP アドレスの中でもっとも大きい IP アドレスを Router-ID として採用します。

○ Connected 再配信

connected ルートを OSPF で配信するかどうかを選択します。「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
　配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
　配信する際のメトリック値を設定します。

○ static ルートの再配信

static ルートを OSPF で配信するかどうかを選択します。**IPsec ルートを再配信する場合も、この設定を「有効」にする必要があります。**

「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
　配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
　配信する際のメトリック値を設定します。

○ RIP ルートの再配信

RIP が学習したルート情報を OSPF で配信するかどうかを選択します。「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
　配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
　配信する際のメトリック値を設定します。

○ Administrative Distance 設定

ディスタンス値を設定します。OSPF と他のダイナミックルーティングを併用していて同じサブネットを学習した際に、この値の小さい方のダイナミックルートを経路として採用します。

○ External ルート Distance 設定

OSPF 以外のプロトコルで学習した経路のディスタンス値を設定します。

○ Inter-area ルート Distance 設定

エリア間の経路のディスタンス値を設定します。

○ intra-area ルート Distance 設定

エリア内の経路のディスタンス値を設定します。

III. OSPF の設定

○ Default-information
デフォルトルートを OSPF で配信するかどうかを選択します。

「送信する」の場合、ルータがデフォルトルートを持っていれば送信されますが、たとえば PPPoE セッションが切断しでデフォルトルート情報がなくなってしまったときは配信されなくなります。
「常に送信」の場合、デフォルトルートの有無にかかわらず、自分にデフォルトルートを向けるように、OSPF で配信します。
「送信する」「常に送信する」の場合は、以下の 2 項目についても設定します。

a. メトリックタイプ
配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
配信する際のメトリック値を設定します。

○ SPF 計算 Delay 設定
LSU を受け取ってから SPF 計算をする際の遅延(delay)時間を設定します。

○ 2 つの SPF 計算の最小間隔設定
連続して SPF 計算をおこなう際の間隔を設定します。

○バックアップ切替え監視対象 Remote Router-ID 設定

OSPF Helloによるバックアップ回線切り替え機能を使用する際に、Neighbor が切れたかどうかをチェックする対象のルータを判別するために、対象のルータの IP アドレスを設定します。
バックアップ機能を使用しない場合は、設定する必要はありません。

入力後は「設定」をクリックしてください。

III．OSPF の設定

◆インタフェース設定

各インタフェースごとの OSPF 設定を行ないます。

設定画面上部の「インタフェース設定」をクリックして設定します。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

○インタフェース名
設定するインタフェースを選択します。

○ Passive-Interface 設定
インタフェースが該当するサブネット情報を OSPF で配信し、かつ、このサブネットには OSPF 情報を配信したくないという場合に「有効」を選択します。

○コスト値設定
コスト値を設定します。

○帯域設定
帯域設定をおこないます。この値をもとにコスト値を計算します。コスト値＝ 100Mbps/ 帯域 kbps です。コスト値と両方設定した場合は、コスト値設定が優先されます。

○ Hello インターバル設定
Hello パケットを送出する間隔を設定します。

○ Dead インターバル設定
Dead タイムを設定します。

○ Retransmit インターバル設定
LSA の送出間隔を設定します。

○ Transmit Delay 設定
LSU を送出する際の遅延間隔を設定します。

○認証パスワード設定
simple パスワード認証を使用する際のパスワードを設定します。

○ MD5 KEY-ID 設定(1)
MD5 認証使用時の KEY ID を設定します。

○ MD5 パスワード設定(1)
エリア内で MD5 認証を使用する際の MD5 パスワードを設定します。

○ MD5 KEY-ID 設定(2)
○ MD5 パスワード設定(2)
MD5 KEY-ID とパスワードは 2 つ同時に設定可能です。その場合は(2)に設定します。

○ Priority 設定
DR、BDR の設定の際に使用する priority を設定します。priority 値が高いものが DR に、次に高いものが BDR に選ばれます。0 を設定した場合は DR、BDR の選定には関係しなくなります。

DR、BDR の選定は、priority が同じであれば、IP アドレスの大きいものが DR、BDR になります。

○ MTU-Ignore 設定
DBD 内の MTU 値が異なる場合、Full の状態になることはできません(Exstart になる)。
どうしても MTU を合わせることができないときには、この MTU 値の不一致を無視して Neighbor (Full)を確立させるための MTU-Ignore を「有効」にしてください。

入力後は「設定」をクリックしてください。

III. OSPF の設定

設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。

	インタフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Priority	MTU ignore	Configure
1	eth0	on	10	1000000	10	40	5	1	century	150	centurysystems	50	off	Edit,Remove

「Configure」項目の「Edit」「Remove」をクリックすることで、それぞれ設定内容の「編集」と設定の「削除」をおこなえます。

◆ステータス表示

OSPF の各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。

◯ OSPF データベース表示
LinkState 情報が表示されます。

◯ネイバーリスト情報の表示
現在のネイバー状態が表示されます。

◯ OSPF ルーティングテーブル情報の表示
OSPF ルーティング情報が表示されます。

◯ OSPF 統計情報の表示
SPF の計算回数や Router ID などが表示されます。

◯インタフェース情報の表示
現在のインタフェースの状態が表示されます。

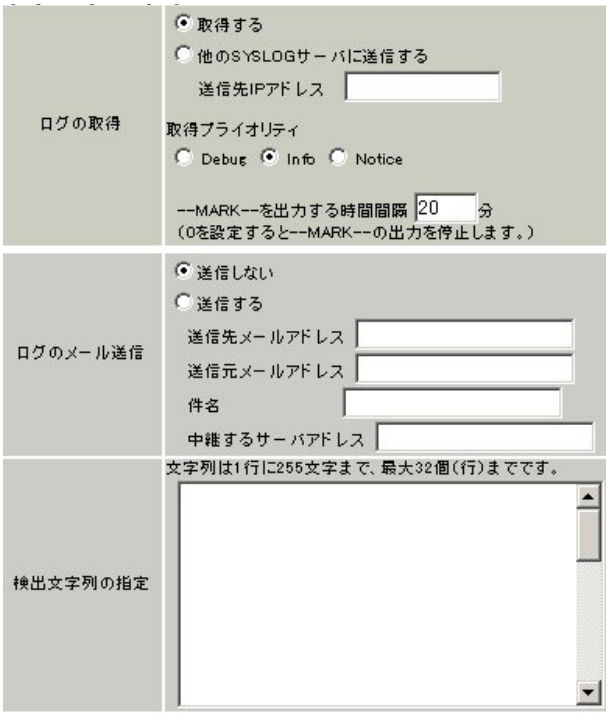
第 15 章

SYSLOG 機能

syslog 機能の設定

XR-410 は、syslog を出力・表示することが可能です。また、他の syslog サーバに送出することもできます。さらに、ログの内容を電子メールで送ることもできます。

Web 設定画面「各種サービスの設定」->「SYSLOG サービス」をクリックして、以下の画面から設定



<syslog 機能設定>

○「ログの取得」項目で設定します。

「取得する」
XR-410 で syslog を取得する場合に選択します。

「他の syslog サーバに送信する」
syslogを他のサーバに送信するときに選択します。このとき、syslog サーバの IP アドレスを指定します。

「取得プライオリティ」
ログ内容の出力レベルを指定します。プライオリティの内容は以下のようになります。

- Debug：デバッグ時に有益な情報
- Info：システムからの情報
- Notice：システムからの通知

「--MARK-- を出力する時間間隔」
syslog が動作していることを表す「--MARK--」ログを送出する間隔を指定します。
初期設定は 20 分です。

XR-410本体に記録しておけるログの容量には制限があります。継続的にログを取得される場合は外部の syslog サーバにログを送出するようにしてください。

<ログメール機能設定>

○ログの内容を電子メールで送信したいときの設定です。「ログメールの送信」項目で設定します。

ログメール機能を使うときは「送信する」を選択し、「ログメッセージ送信先のメールアドレス」を指定します。さらに、
　「ログメッセージ送信元のメールアドレス」
　「件名」
　「中継するサーバアドレス」
を任意で指定できます。「件名」は半角英数字のみ使用できます。

何も指定しないときは
　送信元アドレス「root@localdomain.co.jp」
　件名は無し
で送信されます。

「中継するメールサーバのアドレス」は、お知らせメールを中継する任意のメールサーバを設定します。IP アドレス、ドメイン名のどちらでも設定できます。ただしドメイン名で指定するときは、下記の記述で設定してください。

<入力形式>　**@ <ドメイン名>**
<入力例>　　@mail.xxxxxx.co.jp

(次ページに続きます)

syslog 機能の設定

○検出文字列の指定
ここで指定した文字列が含まれるログをメールで送信します。検出文字列には、pppd、IP、DNS など、ログ表示に使用される文字列を指定してください。なお、文字列の記述に正規表現は使用できません。**文字列を指定しない場合はログメールは送信されません。**

文字列の指定は、1 行につき 256 文字まで、かつ最大 32 行までです。空白・大小文字も判別します。一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。**なお「検出文字列の指定」項目は、「ログメール機能」のみ有効です。**

最後に「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

ファシリティと監視レベルについて
XR-410 シリーズで設定されている syslog のファシリティ・監視レベルおよび出力先は以下のようになっています。

[ファシリティ：監視レベル]
***.info;mail.none;news.none;authpriv.none**

[出力先]
/var/log/messages

第 16 章

帯域制御(QoS)機能

第 16 章 帯域制御(QoS)機能

Ⅰ.QoS 機能の概要

◆QoS 機能について

QoS とは”Quality of Service”の略で、本来はアプリケーションのサービス品質を一定で維持することを意味しています。これが転じて、特定のアプリケーションに対してネットワークの帯域を割り当てる機能のことを QoS と呼びます。

一般的に、ネットワークにおける通信では FTP やストリーミングなどで同時に大量のパケットが伝送されると、各機器において通信のレスポンスが悪くなってしまいます(アクセスが増えるごとに、セッションあたりの帯域が狭くなっていきます)。

そこでアプリケーション毎に占有できる帯域幅を調整することで、レスポンスの低下を防ぎます。たとえば FTP に 64kbps、その他に 64kbps という帯域幅を設定すれば、FTP アクセスの際には常に最大 64kbps の帯域を使用してアクセスできるようになります。

XR-410 では、**Ethernet ポートから送出されるトラフィックについて帯域を制御**します。

PPP/PPPoE 論理ポートについて帯域制御を行うことはできませんので、例えば PPPoE 接続について帯域制御をおこなう場合も Ether0 ポート側で制御してください。

また送信元 / あて先の IP アドレス・ポート番号を指定して制御できます。

11. QoS 機能の設定

Web 設定画面「各種サービスの設定」→「帯域制御(QoS)サービス」をクリックして、以下の画面から設定します。

○制御する帯域幅
この条件に合致するパケットに割り当てる帯域幅を設定します。kbps 単位で設定します。
本装置の各 Ethernet ポートから送信されるパケットが帯域制御の対象となります。

○送信元 IP アドレス

送信元ホストの IP アドレスまたはネットワークアドレスを設定します。

範囲で設定することはできません。
< 入力例 >
ホスト単体の場合　***192.168.0.1/32***（”/32”を付ける）
ネットワーク単位の場合　***192.168.0.0/24***（”/マスクビット値”を付ける）

○送信元ポート番号

送信元ポート番号を設定します。範囲で設定することはできません。

○あて先 IP アドレス

あて先ホストの IP アドレスまたはネットワークアドレスを設定します。

範囲で設定することはできません。

入力方法は、送信元 IP アドレスの場合と同じです。

○あて先ポート番号

あて先ポート番号を設定します。範囲で設定することはできません。

○インターフェース

帯域制御をおこなうインターフェースを選択します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
一覧の ”No.” が赤いときは、その番号の設定が正しくないことを示しています。再度設定し直してください。

帯域制御をおこなう場合は、「QoS 機能の開始 / 停止」項目で QoS 機能を有効にします。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。

設定の削除方法

一覧の「削除」ラジオボックスにチェックして「設定 / 削除の実行」をクリックすると、その設定が削除されます。

第17章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

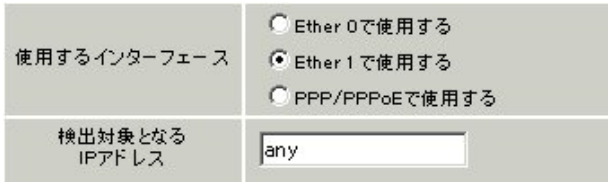
攻撃検出機能とは、外部から LAN への侵入や XR-410 を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。検出方法には、統計的な面から異常な状態を検出する方法やパターンマッチング方法などがあります。XR-410 ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。ホスト単位の他、ネットワーク単位で監視対象を設定できます。

ログの出力

攻撃検出ログも、システムログの中に統合されて出力されますので、「システム設定」内の「ログの表示」やログメール機能で、ログを確認してください。

攻撃検出機能の設定

Web 設定画面「各種サービスの設定」→「攻撃検出サービス」をクリックして、以下の画面で設定します。



○使用するインターフェース
DoS の検出をおこなうインターフェースを選択します。PPPoE/PPP 接続しているインタフェースで検出する場合は「PPP/PPPoE で使用する」を選択してください。

○検出対象となる IP アドレス
攻撃を検出したいホストの IP アドレスか、ネットワークアドレスを指定します。

< 入力例 >
ホスト単体の場合　***192.168.0.1/32***（”/32 ”を付ける）
ネットワーク単位の場合　***192.168.0.0/24***（”/マスクビット値 ”を付ける）

「any」と入力すると、すべてのホストが検出対象となります。そのため通常のアクセスも攻撃として誤検知する場合があります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

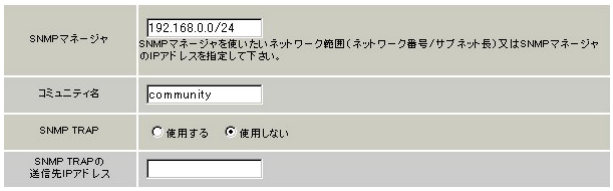
第 18 章

SNMP エージェント機能

SNMP エージェント機能の設定

SNMP エージェントを起動すると、SNMP マネージャから XR-410 の MIB Ver.2(RFC1213)の情報を取得することができます。

Web 設定画面「各種サービス設定」→「SNMP サービス」をクリックして、以下の画面で設定します。



○ SNMP マネージャ
SNMP マネージャを使いたいネットワーク範囲（ネットワーク番号 / サブネット長）又は SNMP マネージャの IP アドレスを指定します。

○コミュニティ名
任意のコミュニティ名を指定します。
ご使用の SNMP マネージャの設定に合わせて入力してください。

○ SNMP TRAP
「使用する」を選択すると、SNMP TRAP を送信できるようになります。

○ SNMP TRAP の送信先 IP アドレス
SNMP TRAP を送信する先(SNMP マネージャ)の IP アドレスを指定します。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

第 19 章

NTP サービス

NTP サービスの設定方法

XR-410 は、NTP クライアント / サーバ機能を持っています。インターネットを使った時刻同期の手法の一つである NTP(Network Time Protocol)を用いて NTP サーバと通信を行い、時刻を同期させることができます。

Web 設定画面「各種サービスの設定」→「NTP サービス」をクリックして以下の画面で NTP 機能の設定をします。

○ NTP サーバの IP アドレスもしくは URL を「設定「設定 1」もしくは「設定 2」に入力します（NTP サーバの場所は２箇所設定できます)。これにより、XR-410 が NTP クライアント / サーバとして動作できます。

NTP サーバの IP アドレスもしくは URL を入力しない場合は、XR-410 は NTP サーバとしてのみ動作します。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

基準 NTP サーバについて

基準となる NTP サーバには以下のようなものがあります。

・高エネルギー物理学研究所:
　　gps.kek.jp (130.87.32.71)
・東京大学:
　　ntp.nc.u-tokyo.ac.jp (130.69.251.23)

(注) サーバをドメイン名で指定するときは、各種サービス設定の「DNS サーバ」を起動しておきます。

NTP サービスの動作について

NTP サービスが起動したときは 64 秒間隔で NTP サーバとポーリングをおこないます。その後は 64 秒から 1024 秒の間で NTP サーバとポーリングをおこない、時刻のずれを徐々に補正していきます。

NTP クライアントの設定方法

各ホスト / サーバーを NTP クライアントとして XR-410 と時刻同期させる方法は、OS により異なります。

○ Windows 9x/Me/NT の場合
これらの OS では NTP プロトコルを直接扱うことができません。フリーウェアの NTP クライアント・アプリケーション等を入手してご利用下さい。

○ Windows 2000 の場合
「net time」コマンドを実行することにより時刻の同期を取ることができます。コマンドの詳細については Microsoft 社にお問い合わせ下さい。

○ Windows XP の場合
Windows 2000 と同様のコマンドによるか、「日付と時刻のプロパティ」で NTP クライアントの設定ができます。詳細については Microsoft 社にお問い合わせください。

○ Macintosh の場合
コントロールパネル内の NTP クライアント機能で設定してください。詳細は Apple 社にお問い合わせください。

○ Linux の場合
Linux 用 NTP サーバをインストールして設定してください。詳細は NTP サーバの関連ドキュメント等をご覧下さい。

第 20 章

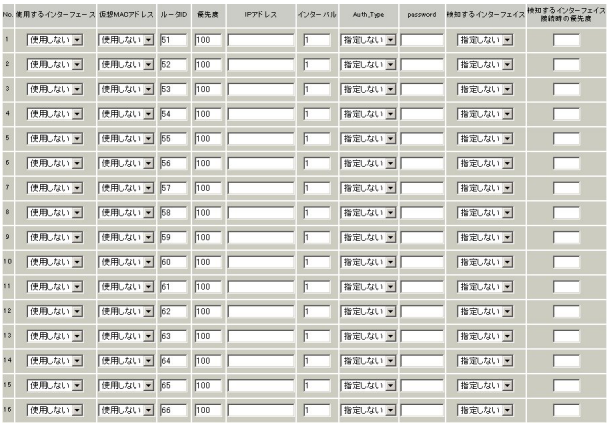
VRRP 機能

第 18 章 VRRP サービス

Ⅰ.VRRP の設定方法

VRRP は動的な経路制御ができないネットワーク環境において、複数のルータのバックアップ(ルータの多重化)をおこなうためのプロトコルです。

「各種サービスの設定」→「VRRP サービス」をクリックして以下の画面で VRRP サービスの設定をします。



○使用するインタフェース
VRRP を作動させるインタフェースを選択します。

○仮想 MAC アドレス
VRRP 機能を運用するときに、仮想 MAC アドレスを使用する場合は「使用する」を選択します。「使用しない」設定の場合は、本装置の実 MAC アドレスを使って VRRP が動作します。

○ルータ ID
VRRP グループの ID を入力します。
他の設定 No. と同一のルータ ID を設定すると、同一の VRRP グループに属することになります。
ID が異なると違うグループと見なされます。

○優先度
VRRP グループ内での優先度を設定します。数字が大きい方が優先度が高くなります。
優先度の値が最も大きいものが、VRRP グループ内での「マスタールータ」となり、他のルータは「バックアップルータ」となります。
1～255 の間で指定します。

○ IP アドレス
VRRP ルータとして作動するときの仮想 IP アドレスを設定します。
VRRP を作動させている環境では、各ホストはこの仮想 IP アドレスをデフォルトゲートウェイとして指定してください。

○インターバル
VRRP パケットを送出する間隔を設定します。単位は秒です。1～255 の間で設定します。

VRRP パケットの送受信によって、VRRP ルータの状態を確認します。

○ Auth_Type
認証形式を選択します。「PASS」または「AH」を選択できます。

○ Password
認証を行なう場合のパスワードを設定します。半角英数字で 8 文字まで設定できます。
Auth_Type を「指定しない」にした場合は、パスワードは設定しません。

○検知するインターフェース
PPP/PPPoE で接続しているときに、PPP/PPPoE インタフェース(ppp0)でもリンク状態を検知させたいときには ”ppp0 ” を選択してください。

○検知するインターフェース接続時の優先度
”ppp0 ” も検知するインターフェースとしたときの VRRP グループ内での優先度を設定します。

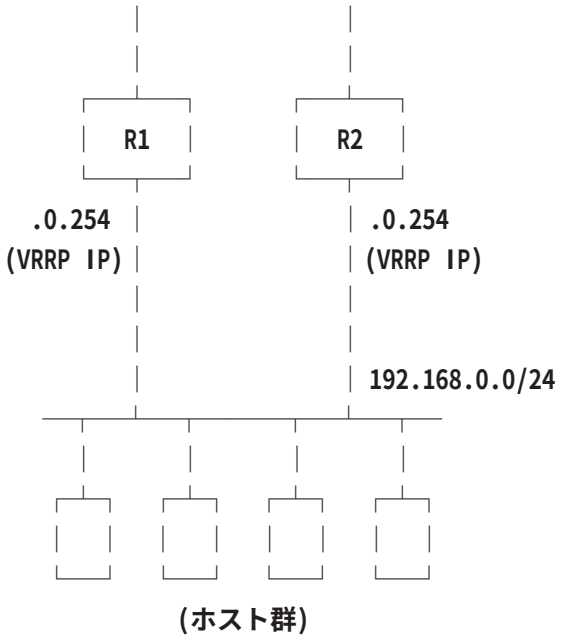
入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合には、サービスの再起動をおこなってください。**

ステータスの表示
VRRP 機能設定画面上部にある「現在の状態」をクリックすると、VRRP 機能の動作状況を表示するウィンドウがポップアップします。

11.VRRP の設定例

下記のネットワーク構成で VRRP サービスを利用するときの設定例です。

ネットワーク構成



設定条件

・ルータ「R1」をマスタルータとする。
・ルータ「R2」をバックアップルータとする。
・ルータの仮想 IP アドレスは「192.168.0.254」
・「R1」「R2」ともに、Ether0 インタフェースで VRRP を作動させる。
・各ホストは「192.168.0.254」をデフォルトゲートウェイとする。
・VRRP ID は「1」とする。
・インターバルは 1 秒とする。
・認証は行なわない。

ルータ「R1」の設定例

ルータ「R2」の設定例

ルータ「R1」が通信不能になると、「R2」が「R1」の仮想 IP アドレスを引き継ぎ、ルータ「R1」が存在しているように動作します。

第 21 章

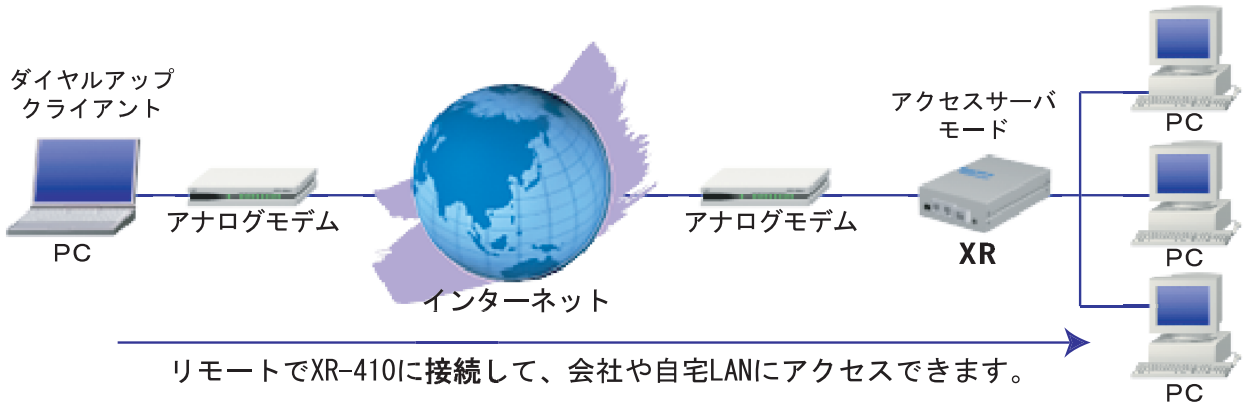
アクセスサーバ機能

第 21 章 アクセスサーバ機能

Ⅰ．アクセスサーバ機能について

アクセスサーバとは、電話回線などを使った外部からの接続要求を受けて、LAN に接続する機能です。例えば、アクセスサーバとして設定した XR-410 を会社に設置すると、モデムを接続した外出先のコンピューターから会社の LAN に接続できます。これは、モバイルコンピューティングや在宅勤務を可能にします。クライアントはモデムによる PPP 接続を利用できるものであれば、どのような PC でもかまいません。この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

セキュリティは、ユーザー ID・パスワード認証によって確保します。ユーザー ID・パスワードは、最大 5 アカウント分を登録できます。



XR-410 のリモートアクセス機能を使う場合、リモートアクセスを受ける側のホストのデフォルトルートが XR-410 に向いている必要があります。

11．XR-410 とアナログモデム /TA の接続

リモートアクセス機能を設定する前に、XR-410 とアナログモデムや TA を接続します。以下のように接続してください。

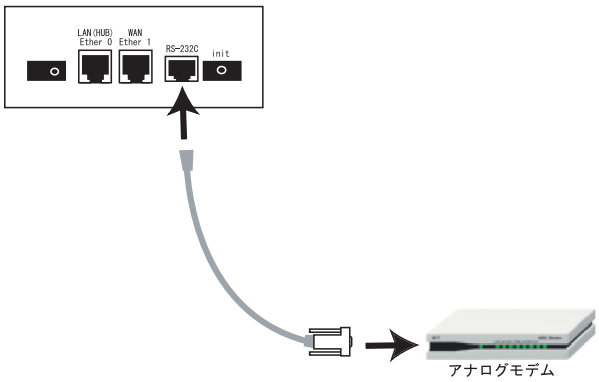
◆アナログモデム /TA の接続

1 XR-410 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

2 変換アダプタのコネクタを、アナログモデム /TA のシリアルポートに接続してください。シリアルポートのコネクタが 25 ピンタイプの場合は別途、変換コネクタをご用意ください。

3 全ての接続が完了しましたら、モデム /TA の電源を投入してください。

接続図



III．アクセスサーバ機能の設定

Web 設定画面「各種サービスの設定」→「アクセスサーバ」をクリックして設定します。

○アクセスサーバ
アクセスサーバ機能の使用 / 不使用を選択します。

○アクセスサーバ(本装置)の IP アドレス
リモートアクセスされた時の XR-410 自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。***なお、サブネットのマスクビット値は 24 ビット(255.255.255.0)に設定されています。***

○クライアントの IP アドレス
XR-410 にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

○モデムの速度
XR-410 とモデムの間の通信速度を選択します。

○着信のための AT コマンド
モデムが外部から着信する場合、AT コマンドが必要な場合があります。その場合は、ここで AT コマンドを入力してください。コマンドについては、各モデムの説明書をご確認ください。

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

外部からリモートアクセスする場合の、ユーザーアカウントとパスワードを登録してください。そのまま、リモートアクセス時のユーザーアカウント・パスワードとなります。5 アカウントまで登録しておけます。

入力後、「設定の保存」をクリックしてください。設定が反映されます。
アカウント設定覧の「削除」ラジオボックスにチェックして「設定 / 削除の実行」をクリックすると、その設定が削除されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。設定後は、外部からダイヤルアップ接続を行なってください。

※外部からダイヤルアップ接続されていないときには、「各種サービスの設定」画面の「アクセスサーバ」が「待機中」の表示となります。

第 22 章

スタティックルーティング

スタティックルーティング設定

XR-410 は、最大 256 エントリのスタティックルートを登録できます。

Web 設定画面「スタティックルート設定」をクリックして、以下の画面から設定します。

入力方法

○ホスト / ネットワーク
ルーティング先が、単一ホストかネットワークかを選択します。

○アドレス
あて先ホストのアドレス、またはネットワークアドレスを入力します。

○ネットマスク
あて先ネットワークのサブネットマスクを入力します。IP アドレス形式で入力してください。

入力例 ： ***255.255.255.248*** (29ビットマスク)

また、あて先アドレスを単一ホストで指定した場合には、「255.255.255.255」と入力します。
あて先をドメイン名でしてした場合はネットマスクを入力しません。

○インターフェース
ルーティングをおこなうインターフェースを選択します。あて先ホスト / ネットワークがある側のインターフェースを選択します。
また「指定なし」を選択すると、システムが自動的に割り当てるようになります。

○ gre No.
インターフェースで「GRE」を選択した場合、どの GRE 設定を使うか、GRE の設定番号を指定します。GRE の設定については第 27 章をご参照ください。

○ゲートウェイ
ルーティングパケットを中継するルータのアドレスを入力します。XR-410 の上位ルータのアドレス等になります。

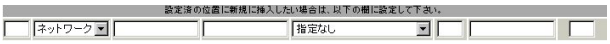
○ディスタンス
経路選択の優先順位を指定します。1 ～ 255 の間で指定します。値が低いほど優先度が高くなります。
スタティックルートのデフォルトディスタンス値は 1 です。
ディスタンス値を変更することで、フローティングスタティックルート設定とすることも可能です。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

スタティックルーティング設定

設定を挿入する

ルーティング設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。
最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。



設定を削除する

ルーティング設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

デフォルトルートを設定する

スタティックルート設定でデフォルトルートを設定するときは、「アドレス」と「ネットマスク」項目をいずれも ”0.0.0.0 ” として設定してください。

ルーティング情報を確認する

現在のルーティング情報を確認するには、設定画面上部にある「経路情報表示」をクリックします。ウィンドウがポップアップし、経路情報が確認できます。
” inactive ” と表示されている経路は、その時点では有効な経路ではなく、無視されます。

表示されていないものに関しては、正しい設定ではありません。設定をご確認のうえ、再度設定してください。

第 23 章

ソースルーティング

第 23 章　ソースルーティング

ソースルーティング設定

通常のダイナミックルーティングおよびスタティックルーティングでは、パケットのあて先アドレスごとにルーティングを行ないますが、ソースルーティングはパケットの送信元アドレスをもとにルーティングをおこないます。

このソースルート機能を使うことで、外部へアクセスするホスト / ネットワークごとにアクセス回線を選択することができますので、複数のインターネット接続をおこなって負荷分散が可能となります。

ソースルート設定は、設定画面「ソースルート設定」でおこないます。

1 はじめに、ソースルートのテーブル設定をおこないます。「ソースルートのテーブル設定へ」をクリックしてください。

○ IP
デーフォルトゲートウェイ(上位ルータ)の IP アドレスを設定します。必ず明示的に設定しなければなりません。

○ DEVICE
デフォルトゲートウェイが存在する回線に接続しているインタフェースのインタフェース名を設定します(情報表示で確認できます。” eth0 ” や ” ppp0 ” などの表記のものです)。省略することもできます。

設定後は「設定の保存」をクリックします。

2 画面右上の「ソースルートのルール設定へ」をクリックします。

○送信元ネットワークアドレス
送信元のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、
　ネットワークアドレス / マスクビット値
の形式で設定してください。

○送信先ネットワークアドレス
送信先のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、
　ネットワークアドレス / マスクビット値
の形式で設定してください。FQDN での設定も可能です。

○ソースルートのテーブル No.
使用するソースルートテーブルの番号(1 ～ 8)を設定します。

最後に「設定の保存」をクリックして設定完了です。

※送信元ネットワークアドレスをネットワークアドレスで指定した場合、そのネットワークに XR-410 のインタフェースが含まれていると、設定後は XR-410 の設定画面にアクセスできなくなります。

< 例 >Ether0 ポートの IP アドレスが 192.168.0.254 で、送信元ネットワークアドレスを 192.168.0.0/24 と設定

第 24 章

NAT 機能

第 24 章　NAT 機能

Ⅰ．XR-410 の NAT 機能について

NAT(Network Address Translation)は、プライベートアドレスをグローバルアドレスに変換してインターネットにアクセスできるようにする機能です。また 1 つのプライベートアドレス・ポートと、1 つのグローバルアドレス・ポートを対応させて、インターネット側から LAN のサーバへアクセスさせることもできます。

XR-410 は以下の 3 つの NAT 機能をサポートしています。

◆ IP マスカレード機能
複数のプライベートアドレスを、ある 1 つのグローバルアドレスに変換する機能です。グローバルアドレスは XR-410 のインターネット側ポートに設定されたものを使います。また LAN のプライベートアドレス全てが変換されることになります。この機能を使うと、グローバルアドレスを 1 つしか持っていなくても複数のコンピュータからインターネットにアクセスすることができるようになります。

なお IP マスカレード(NAT 機能)では、プライベートアドレスからグローバルアドレスだけではなく、プライベートアドレスからプライベートアドレス、グローバルアドレスからグローバルアドレスの変換も可能です。IP マスカレード機能については、「インターフェース設定」もしくは「PPP/PPPoE 接続」の接続設定画面で設定します。

◆送信元 NAT 機能
IP マスカレードとは異なり、プライベートアドレスをどのグローバル IP アドレスに変換するかをそれぞれ設定できるのが送信元 NAT 機能です。例えば、プライベートアドレスＡをグローバルアドレスＸに、プライベートアドレスＢをグローバルアドレスＹに、プライベートアドレスＣからＦをグローバルアドレスＺに変換する、といった設定が可能になります。IP マスカレード機能を設定せずに送信元 NAT 機能だけを設定した場合は、送信元 NAT 機能で設定されたアドレスを持つコンピュータしかインターネットにアクセスできません。

◆バーチャルサーバ機能
インターネット上から LAN 上のサーバ等にアクセスさせることができる機能です。通常はインターネット側から LAN へアクセスする事はできませんが、送信先グローバルアドレスをプライベートアドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスできているかのようにすることができます。設定上ではプライベートアドレスとグローバルアドレスを 1 対 1 で関連づけます。また同時に、プロトコルと TCP/UDP ポート番号も指定しておきます。ここで指定したプロトコル・TCP/UDP ポート番号でアクセスされた時にグローバルアドレスからプライベートアドレスへ変換され、LAN 上のサーバに転送されます。

これらの NAT 機能は同時に設定・運用が可能です。

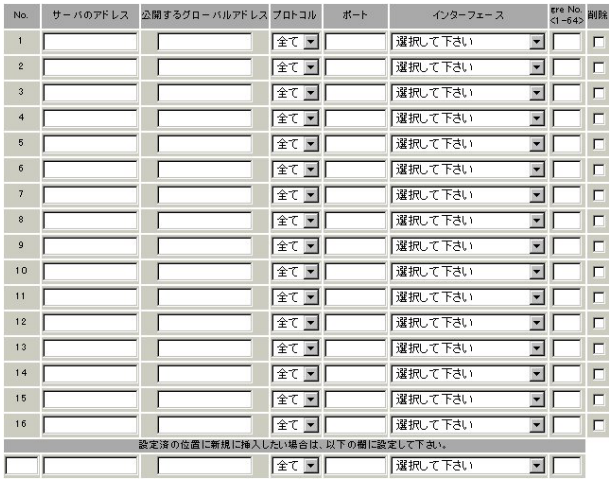
NetMeeting や各種 IM、ネットワークゲームなど、独自のプロトコル・ポートを使用しているアプリケーションについては、NAT 機能を使用すると正常に動作しない場合があります。原則として、NAT を介しての個々のアプリケーションの動作についてはサポート対象外とさせていただきます。

11．バーチャルサーバ設定

NAT 環境下において、LAN からサーバを公開するときなどの設定をおこないます。

設定方法

Web 設定画面「NAT 設定」→「バーチャルサーバ」をクリックして、以下の画面から設定します。



○サーバのアドレス
インターネットに公開するサーバの、プライベート IP アドレスを入力します。

○公開するグローバルアドレス
サーバのプライベート IP アドレスに対応させるグローバル IP アドレスを入力します。インターネットからはここで入力したグローバル IP アドレスでアクセスします。
プロバイダから割り当てられている IP アドレスが一つだけの場合は、ここは空欄にします。

○プロトコル
サーバのプロトコルを選択します。

○ポート
サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を ":" で結びます。
<例> ポート 20 番から 21 番を指定する → ***20:21***

○インターフェース
インターネットからのアクセスを受信するインターフェースを選択します。インターネットに接続しているインターフェースを選択してください。
PPP/PPPoE で接続する場合は、「PPP/PPPoE」を選択してください。

○ gre No.
インターフェースで「GRE」を選択した場合、どの GRE 設定を使うか、GRE の設定番号を指定します。GRE の設定については第 28 章をご参照ください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
"No." 項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定を削除する

バーチャルサーバ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

III. 送信元 NAT 設定

設定方法

Web 設定画面「NAT 設定」→「送信元 NAT」をクリックして、以下の画面から設定します。

○送信元のプライベートアドレス
NAT の対象となる LAN 側コンピューターのプライベート IP アドレスを入力します。ネットワーク単位での指定も可能です。

○変換後のグローバルアドレス
プライベート IP アドレスの変換後のグローバル IP アドレスを入力します。送信元アドレスをここで入力したアドレスに書き換えてインターネット(WAN)へアクセスします。

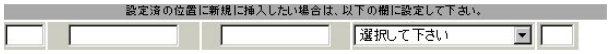
○インターフェース
どのインターフェースからインターネット(WAN)へアクセスするか、インターフェースを選択します。インターネット(WAN)につながっているインターフェースを選択してください。
PPPoE/PPP で接続する場合は、「PPPoE/PPP」を選択してください。

○gre No.
インターフェースで「GRE」を選択した場合、どの GRE 設定を使うか、GRE の設定番号を指定します。GRE の設定については第 27 章をご参照ください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を挿入する

送信元 NAT 設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定を削除する

送信元 NAT 設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

IV. バーチャルサーバの設定例

◆ WWW サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスに TCP のポート 80 番(http)でのアクセスを通す。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・WWW サーバのアドレス「192.168.0.1」
・グローバルアドレスは「211.xxx.xxx.102」のみ

設定画面での入力方法

・あらかじめ IP マスカレードを有効にします。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	grp No. <1-64>
192.168.0.1	211.xxx.xxx.102	tcp	80	Ether1ポート	

設定の解説

No.1 ：
WAN 側から、211.xxx.xxx.102 へポート 80 番(http)でアクセスがあれば、LAN 内のサーバ 192.168.0.1 へ通す。(WAN 側から TCP のポート 80 番以外でアクセスがあっても破棄される)

◆ FTP サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスに TCP のポート 20 番(ftpdata)、21 番(ftp)でのアクセスを通す。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・Ether1 ポートは PPPoE で ADSL 接続する。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・FTP サーバのアドレス「192.168.0.2」
・グローバルアドレスは「211.xxx.xxx.103」のみ

設定画面での入力方法

・あらかじめ IP マスカレードを有効にます。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	grp No. <1-64>
192.168.0.2	211.xxx.xxx.103	tcp	20	PPP/PPPoE－主回線 #1	
192.168.0.2	211.xxx.xxx.103	tcp	21	PPP/PPPoE－主回線 #1	

設定の解説

No.1 ：
WAN 側から、211.xxx.xxx.103 へポート 21 番(ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。
No.2 ：
WAN 側から、211.xx.xx.103 へポート 20 番(ftpdata)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

IV．バーチャルサーバの設定例

◆PPTP サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスにプロトコル「gre」と TCP のポート番号 1723 を通す。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・WAN 側ポートは PPPoE で ADSL 接続する。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・PPTP サーバのアドレス「192.168.0.3」
・割り当てられるグローバルアドレスは 1 つのみ。

設定画面での入力方法

・あらかじめ IP マスカレードを有効にます。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	gre No. <1-64>
192.168.0.3		tcp	1723	PPP/PPPoE－主回線 #1	
192.168.0.3		gre		選択して下さい	

IV. バーチャルサーバの設定例

◆DNS、メール、WWW、FTP サーバを公開する際の NAT 設定例(複数グローバルアドレスを利用)

NAT の条件

- WAN 側からは、LAN 側のメール、WWW,FTP サーバへアクセスできるようにする。
- LAN 内の DNS サーバが WAN と通信できるようにする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続。
- グローバルアドレスは複数使用する。

LAN 構成

- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」
- 送受信メールサーバのアドレス「192.168.0.2
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」
- WWW サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.104」
- 送受信メールサーバに対応させるグローバル IP アドレスは「211.xxx.xxx.105」
- FTP サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.106」
- DNS サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.107」

設定画面での入力方法

1 まず最初に、使用する複数のグローバルアドレスを、仮想インターフェースとして登録します。メニューにある「仮想インターフェース設定」を開き、以下のように設定しておきます。

インターフェース	仮想I/F番号	IPアドレス	ネットマスク
Ether1ポート	1	211.xxx.xxx.104	255.255.255.248
Ether1ポート	2	211.xxx.xxx.105	255.255.255.248
Ether1ポート	3	211.xxx.xxx.106	255.255.255.248
Ether1ポート	4	211.xxx.xxx.107	255.255.255.248

2 IP マスカレードを有効にします。(第 5 章参照)

3 「バーチャルサーバ設定」で以下の様に設定してください。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	pre No. <1-64>
192.168.0.1	211.xxx.xxx.104	tcp	80	Ether1ポート	
192.168.0.2	211.xxx.xxx.105	tcp	25	Ether1ポート	
192.168.0.2	211.xxx.xxx.105	tcp	110	Ether1ポート	
192.168.0.3	211.xxx.xxx.106	tcp	21	Ether1ポート	
192.168.0.3	211.xxx.xxx.106	tcp	20	Ether1ポート	
192.168.0.4	211.xxx.xxx.107	tcp	53	Ether1ポート	
192.168.0.4	211.xxx.xxx.107	udp	53	Ether1ポート	

設定の解説

No.1
WAN 側から 211.xxx.xxx.104 へポート 80 番(http)でアクセスがあれば、LAN 内のサーバ 192.168.0.1 へ通す。

No.2、3
WAN 側から 211.xxx.xxx.105 へポート 25 番(smtp)か 110 番(pop3)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

No.4、5
WAN 側から 211.xxx.xxx.106 へポート 20 番(ftpdata)か 21 番(ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.3 へ通す。

No.6、7
WAN 側から 211.xxx.xxx.107 へ、tcp ポート 53 番(domain)か udp ポート 53 番(domain)でアクセスがあれば LAN 内のサーバ 192.168.0.4 へ通す。

複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インターフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

V. 送信元 NAT の設定例

送信元 NAT 設定では、LAN 側のコンピューターのアドレスをどのグローバルアドレスに変換するかを個々に設定することができます。

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.0.1	61.xxx.xxx.101	PPP/PPPoE－主回線 #1
192.168.0.2	61.xxx.xxx.102	PPP/PPPoE－主回線 #1
192.168.10.0/24	61.xxx.xxx.103	PPP/PPPoE－主回線 #1

例えば上記のような送信元 NAT 設定をおこなうと、

- 送信元アドレス 192.168.0.1 を 61.xxx.xxx.101 に変換して WAN へアクセスする
- 送信元アドレス 192.168.0.2 を 61.xxx.xxx.102 に変換して WAN へアクセスする
- 送信元アドレスとして 192.168.0.0/24 からのアクセスを 61.xxx.xxx.103 に変換して WAN へアクセスする

という設定になります。

送信元のアドレスは、ホスト単位かネットワーク単位で指定できます。範囲指定はできません。
ネットワークで指定するときは、以下のように設定して下さい。
　＜設定例＞　***192.168.254.0/24***

PPPoE 接続時に複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インターフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細は RFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

第 25 章

パケットフィルタリング機能

第 25 章 パケットフィルタリング機能

1. 機能の概要

XR-410はパケットフィルタリング機能を搭載しています。パケットフィルタリング機能を使うと、以下のようなことができます。

- 外部から LAN に入ってくるパケットを制限する。
- LAN から外部に出ていくパケットを制限する。
- XR-410 自身が受信するパケットを制限する。
- XR-410 自身から送信するパケットを制限する。
- ゲートウェイ認証機能を使用しているときにアクセス可能にする

またフィルタリングは以下の情報に基づいて条件を設定することができます。

- 送信元 / あて先 IP アドレス
- プロトコル(TCP/UDP/ICMP など)
- 送信元 / あて先ポート番号
- 入出力方向(入力 / 転送 / 出力)
- インターフェース

パケットフィルタリング機能を有効にすると、パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元やあて先の IP アドレス、プロトコルの種類(TCP/UDP/ICMP など)、ポート番号に基づいてパケットを通過させたり破棄させることができます。

このようなパケットフィルタリング機能は、コンピューターやアプリケーション側の設定を変更する必要がないために、個々のコンピューターでパケットフィルタの存在を意識することなく、簡単に利用できます。

11.XR-410 のフィルタリング機能について

XR-410 は、以下の 4 つの基本ルールについてフィルタリングの設定をおこないます。

- **転送(forward)**
- **入力(input)**
- **出力(output)**
- **ゲートウェイ認証フィルタ**

◆転送(forward)フィルタ
LAN からインターネットへのアクセスや、インターネットから LAN 内サーバへのアクセス、LAN から LAN へのアクセスなど、XR-410 で内部転送する(XR-410がルーティングする)アクセスを制御するという場合には、この転送ルールにフィルタ設定をおこないます。

◆入力(input)フィルタ
外部から XR-410 自身に入ってくるパケットに対して制御します。インターネットや LAN から XR-410 へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定をおこないます。

◆出力(output)フィルタ
XR-410 内部からインターネットや LAN などへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。
パケットが「転送されるもの」か「XR-410 自身へのアクセス」か「XR-410 自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

◆ゲートウェイ認証フィルタ
「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。ゲートウェイ認証を必要とせずに外部と通信可能にするフィルタ設定をおこないます。ゲートウェイ認証機能については第 27 章をご覧下さい。

各ルール内のフィルタ設定は先頭から順番にマッチングされ、最初にマッチした設定がフィルタとして動作することになります。逆に、マッチするフィルタ設定が見つからなければそのパケットはフィルタリングされません。

本製品の工場出荷設定では、Ether0 ポート以外はステートフルパケットインスペクション機能が有効になっています。この機能により、Ether0 ポート以外から XR-410 自信、また LAN 内へのアクセスは一切できないようになっています。

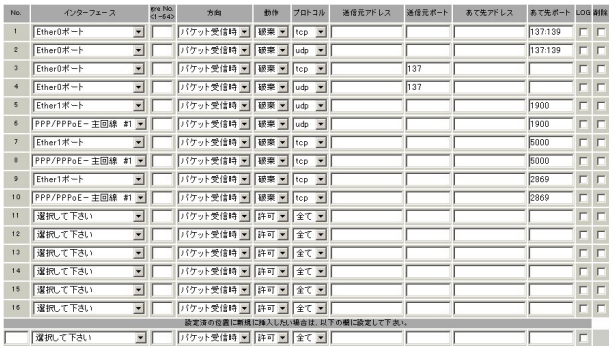
unnumbered 接続やバーチャルサーバ機能によるサーバ公開を運用される場合は、ステートフルパケットインスペクション機能を無効にするかパケットフィルタリングの設定を行い、外部から LAN へのアクセスを許可する設定を行ってください。

III. パケットフィルタリングの設定

入力・転送・出力フィルタの 3 種類ありますが、設定方法はすべて同様となります。

設定方法

Web 設定画面にログインします。「フィルタ設定」→「入力フィルタ」「転送フィルタ」「出力フィルタ」のいずれかをクリックして、以下の画面から設定します。



(画面は「転送フィルタ」です)

○インターフェース
フィルタリングをおこなうインターフェース名を指定します。

○方向
ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。

入力フィルタでは「パケット受信時」、出力フィルタでは「パケット送信時」のみとなります。

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

○プロトコル
フィルタリング対象とするプロトコルを選択します。ポート番号も指定する場合は、ここで必ずプロトコルを選択しておいてください。

○送信元アドレス
フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレス、ドメイン名での指定が可能です。

< 入力例 >
単一の IP アドレスを指定する：
192.168.253.19/32 (" アドレス /32 " の書式)
ネットワーク単位で指定する：
192.168.253.0/24
(" ネットワークアドレス / マスクビット値 " の書式)

○送信元ポート
フィルタリング対象とする、送信元のポート番号を入力します。範囲での指定も可能です。範囲で指定するときは ": " でポート番号を結びます。
< 入力例 > ポート 1024 番から 65535 番を指定する場合。 ***1024:65535***

ポート番号を指定するときは、プロトコルもあわせて選択しておかなければなりません(「全て」のプロトコルを選択して、ポート番号を指定することはできません)

○あて先アドレス
フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレス、FQDN での指定が可能です。
入力方法は、送信元 IP アドレスと同様です。

○あて先ポート
フィルタリング対象とする、送信先のポート番号を入力します。範囲での指定も可能です。指定方法は送信元ポート同様です。

○ LOG
チェックを入れると、そのフィルタ設定に合致したパケットがあったとき、そのパケットの情報を syslog に出力します。許可 / 破棄いずれの場合も出力します。

(次ページに続きます)

III. パケットフィルタリングの設定

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

送信元 / あて先アドレスを FQDN で設定したときは、本装置の DNS サーバ機能が「起動」している必要があります。
また本装置がインターネットに接続できるようになっている必要があります(名前解決をおこなうため)。
本装置を再起動したときなど、タイミングによって名前解決ができずに FQDN での設定が正しく動作しない場合には、本装置がインターネットに接続していることを確認し、「設定の保存」ボタンを再度クリックしてください。

設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定を削除する

フィルタ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

IV. パケットフィルタリングの設定例

◆インターネットから LAN へのアクセスを破棄する設定

本製品の工場出荷設定では、インターネット側から LAN へのアクセスは全て通過させる設定となっていますので、以下の設定をおこない、外部からのアクセスを禁止するようにします。

フィルタの条件

- WAN 側からは LAN 側へアクセス不可にする。
- LAN から WAN へのアクセスは自由にできる。
- XR-410 から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- LAN から WAN へ IP マスカレードをおこなう。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.1」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
Ether1ポート		パケット受信時	許可	tcp				1024:65535
Ether1ポート		パケット受信時	許可	udp				1024:65535
Ether1ポート		パケット受信時	破棄	全て				

「入力フィルタ」で以下のように設定します。

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
Ether1ポート		パケット受信時	許可	tcp				1024:65535
Ether1ポート		パケット受信時	許可	udp				1024:65535
Ether1ポート		パケット受信時	破棄	全て				

フィルタの解説

「転送フィルタ」「入力フィルタ」

No.1：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.2：
上記の条件に合致しないパケットを全て破棄する。

IV. パケットフィルタリングの設定例

◆WWW サーバを公開する際のフィルタ設定例

フィルタの条件

- WAN 側からは LAN 側の WWW サーバにだけアクセス可能にする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続。
- ステートフルインスペクション機能は有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
Ether1ポート		パケット受信時	許可	tcp			192.168.0.1	80
Ether1ポート		パケット受信時	許可	tcp				1024:65535
Ether1ポート		パケット受信時	許可	udp				1024:65535
Ether1ポート		パケット受信時	破棄	全て				

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。

No.2：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.3：
上記の条件に合致しないパケットを全て破棄する。

◆FTP サーバを公開する際のフィルタ設定例

フィルタの条件

- WAN 側からは LAN 側の FTP サーバにだけアクセスが可能にする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- NAT は有効。
- Ether1 ポートは PPPoE 回線に接続する。
- ステートフルインスペクション機能は有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.254」
- FTP サーバのアドレス「192.168.0.2」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.2	21
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.2	20
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp				1024:65535
PPP/PPPoE－主回線 #1		パケット受信時	許可	udp				1024:65535
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て				

フィルタの解説

No.1：
192.168.0.2 のサーバに ftp のパケットを通す。

No.2：
192.168.0.2 のサーバに ftpdata のパケットを通す。

No.3、4：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.5：
上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意下さい。

IV. パケットフィルタリングの設定例

◆WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例

フィルタの条件

- WAN 側からは LAN 側の WWW、FTP、メールサーバにだけアクセスが可能にする。
- DNS サーバが WAN と通信できるようにする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- PPPoE で ADSL に接続する。
- NAT は有効。
- ステートフルインスペクション機能は有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」
- メールサーバのアドレス「192.168.0.2」
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	ere No. (1-64)	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.1	80
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.2	25
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.2	110
PPP/PPPoE－主回線 #1		パケット受信時	許可	udp			192.168.0.3	21
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.3	20
PPP/PPPoE－主回線 #1		パケット受信時	許可	udp			192.168.0.4	53
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp			192.168.0.4	53
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp				1024-65535
PPP/PPPoE－主回線 #1		パケット受信時	許可	udp				1024-65535
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て				

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。

No.2,3：
192.168.0.2 のサーバに SMTP と POP3 のパケットを通す。

No.4,5：
192.168.0.3 のサーバに ftp と ftpdata のパケットを通す。

No.6,7：
192.168.0.4 のサーバに、domain のパケット(tcp,udp)を通す。

No.8、9：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.10：
上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意下さい。

IV. パケットフィルタリングの設定例

◆NetBIOS パケットが外部へ出るのを防止するフィルタ設定

フィルタの条件

・LAN 側から送出された NetBIOS パケットを WAN へ出さない。(Windows での自動接続を防止する)

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス「192.168.0.254」

設定画面での入力方法

「入力フィルタ」

「転送フィルタ」

フィルタの解説

No.1：
　あて先ポートが tcp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.2：
　あて先ポートが udp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.3：
　送信先ポートが tcp の 137 のパケットを Ether0 ポートで破棄する。
No.2：
　送信先ポートが udp の 137 のパケットを Ether0 ポートで破棄する。

◆WAN からのブロードキャストパケットを破棄するフィルタ設定(smurf 攻撃の防御)

フィルタの条件

・WAN 側からのブロードキャストパケットを受け取らないようにする。→ smurf 攻撃を防御する

LAN 構成

・プロバイダから割り当てられたネットワーク空間「210.xxx.xxx.32/28」
・WAN 側は PPPoE 回線に接続する。
・WAN 側ポートの IP アドレス「210.xxx.xxx.33」

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

フィルタの解説

No.1：
　210.xxx.xxx.32(ネットワークアドレス)宛てのパケットを受け取らない。
No.2：
　210.xxx.xxx.32 のネットワークのブロードキャストパケットを受け取らない。

これらの設定例は説明のためのものです。これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意下さい。

IV. パケットフィルタリングの設定例

◆WAN からのパケットを破棄するフィルタ設定 (IP spoofing 攻撃の防御)

フィルタの条件

・WAN 側からの不正な送信元 IP アドレスを持つパケットを受け取らないようにする。
→ IP spoofing 攻撃を受けないようにする。

LAN 構成

・LAN 側のネットワークアドレス
「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

インターフェース	ere No. (1-64)	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	10.0.0.0/8			
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	172.16.0.0/16			
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1,2,3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→ WAN 上にプライベートアドレスは存在しない。

◆外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

・WAN 側からの不正な送信元・送信先 IP アドレスを持つパケットを受け取らないようにする。
→ WAN からの攻撃を受けない・攻撃の踏み台にされないようにする。

LAN 構成

・プロバイダから割り当てられたアドレス空間
「202.xxx.xxx.112/28」
・LAN 側のネットワークアドレス
「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

インターフェース	ere No. (1-64)	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	10.0.0.0/8			
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	172.16.0.0/16			
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て	192.168.0.0/16			
PPP/PPPoE－主回線 #1		パケット受信時	破棄	udp			202.xxx.xxx.112/3	
PPP/PPPoE－主回線 #1		パケット受信時	破棄	全て			202.xxx.xxx.127/3	

「出力フィルタ設定」で以下のように設定します。

インターフェース	ere No. (1-64)	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット送信時	破棄	全て			10.0.0.0/8	
PPP/PPPoE－主回線 #1		パケット送信時	破棄	全て			172.16.0.0/16	
PPP/PPPoE－主回線 #1		パケット送信時	破棄	全て			192.168.0.0/16	

フィルタの解説

入力フィルタの No.1,2,3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→ WAN 上にプライベートアドレスは存在しない。
入力フィルタの No.4：
WAN からのブロードキャストパケットを受け取らない。→ smurf 攻撃の防御
出力フィルタの No.1,2,3：
送信元 IP アドレスが不正なパケットを送出しない。→ WAN 上にプライベートネットワークアドレスは存在しない。

これらの設定例は説明のためのものです。これらのフィルタを設定して安全を確保できることを保証するものではありません。

IV. パケットフィルタリングの設定例

◆PPTP を通すためのフィルタ設定

フィルタの条件

・WAN 側からの PPTP アクセスを許可する。

LAN 構成

・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

インターフェース	gre No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	許可	gre				
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp				1723

フィルタの解説

PPTP では以下のプロトコル・ポートを使って通信します。

・プロトコル「GRE」
・プロトコル「tcp」のポート「1723」

したがいまして、フィルタ設定では上記 2 つの条件に合致するパケットを通す設定をおこなっています。

V. 外部から設定画面にアクセスさせる設定

XR-410 の初期設定では、ステートフルパケットインスペクション機能が有効になっています。そのため、外部から XR-410 の設定画面にアクセスできないようになっています。

しかし、遠隔で XR-410 の設定・制御をおこなう必要がある場合は、「入力フィルタ」で必要な設定をおこなうことで、外部から設定画面にアクセス可能にすることができます。以下は、PPPoE で接続した場合の設定方法です。

1 まず設定画面にログインし、パケットフィルタ設定の「入力フィルタ」画面を開きます。

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

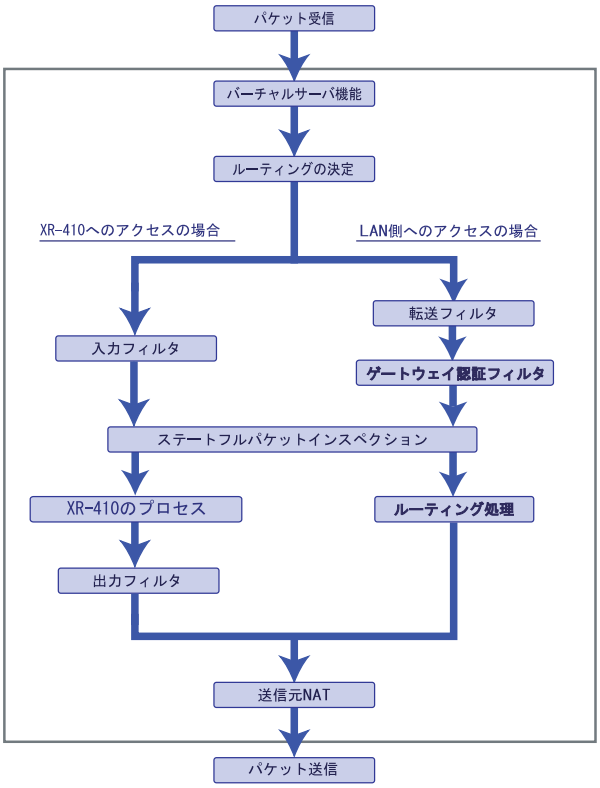
インターフェース	grp No. <1-64>	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
PPP/PPPoE－主回線 #1		パケット受信時	許可	tcp	221.xxx.xxx.105			880

上記設定では、221.xxx.xxx.105 の IP アドレスを持つホストだけが、外部から XR-410 の設定画面へのアクセスが可能になります。

また「送信元アドレス」を空欄にすると、すべてのインターネット上のホストから、XR-410 にアクセス可能になります(**セキュリティ上たいへん危険ですので、この設定は推奨いたしません**)。

補足：NAT とフィルタの処理順序について

XR-410 における、NAT とフィルタリングの処理方法は以下のようになっています。



(図の上部を WAN 側、下部を LAN 側とします。また LAN → WAN へ NAT をおこなうとします。)

・WAN 側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。

・「バーチャルサーバ設定」で静的 NAT 変換したあとに、パケットがルーティングされます。

・XR-410 自身へのアクセスをフィルタするときは「入力フィルタ」、XR-410 自身からのアクセスをフィルタするときは「出力フィルタ」で設定します。

・WAN 側から LAN 側へのアクセスをフィルタするときは「転送フィルタ」で設定します。その場合のあて先アドレスは「(LAN 側の)プライベートアドレス」になります(NAT の後の処理となるため)。

・ステートフルパケットインスペクションだけを有効にしている場合、WAN から LAN、また XR-410 自身へのアクセスはすべて破棄されます。

・ステートフルパケットインスペクションと同時に「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」にある設定が優先して処理されます。

・「送信元 NAT 設定」は、一番最後に参照されます。

・LAN 側から WAN 側へのアクセスの場合も、処理の順序は同様です(最初にバーチャルサーバ設定が参照される)。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。
詳細はRFC1700(Oct．1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

補足：フィルタのログ出力内容について

フィルタ設定画面で「LOG」にチェックを入れると、その設定に合致したパケットの情報を syslog に出力します。出力内容は以下のようになります。

<入力パケットを破棄したときのログ出力例>

```
Jan 25 14:14:07 localhost XR-Filter:  FILTER_INPUT_1 IN=eth0 OUT= MAC=00:80:6d:xx:xx:xx:00:
20:ed:yy:yy:yy:80:00  SRC=192.168.xxx.xxx DST=xxx.xxx.xxx.xxx LEN=40 TOS=00 PREC=0x00 TTL=128
ID=43951 CE DF PROTO=TCP SPT=2526 DPT=880 SEQ=4098235374 ACK=1758964579 WINDOW=48000 ACK
URGP=0
```

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの 1 番目のフィルタで取得されたものです。 FILTER_FORWARD は転送フィルタを意味します。
IN=	パケットを受信したインターフェイスが記されます。
OUT=	パケットを送出したインターフェイスが記されます。なにも記載されていないときは、XR のどのインタフェースからもパケットを送出していないことを表わしています。
MAC=	送信元・あて先の MAC アドレスが記されます。
SRC=	送信元 IP アドレスが記されます。
DST=	送信先 IP アドレスが記されます。
LEN=	パケット長が記されます。
TOS=	TOS bit の状態が記されます。
TTL=	TTL の値が記されます。
ID=	IP の ID が記されます。
PROTO=	プロトコルが記されます。

プロトコルが ICMP の時は、以下のような ICMP 用のメッセージも記されます。

TYPE=0	ICMP のタイプが記されます。
CODE=0	ICMP のコードが記されます。
ID=3961	ICMP の ID が記されます。
SEQ=6656	ICMP のシーケンス番号が記されます。

第 26 章

仮想インターフェース機能

仮想インターフェースの設定

主にバーチャルサーバ機能を利用する場合に、仮想インタフェースを設定します。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

○インターフェース
仮想インターフェースを作成するインターフェースを選択します。
PPP/PPPoE で接続するインターフェースに設定するときは、「PPP/PPPoE」インタフェースを選択します。

○仮想 I/F 番号
作成するインターフェースの番号を指定します。
自由に設定できます。

○ IP アドレス
作成するインターフェースの IP アドレスを指定します。

○ネットマスク
作成するインターフェースのネットマスクを指定します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を削除する

仮想インターフェース設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

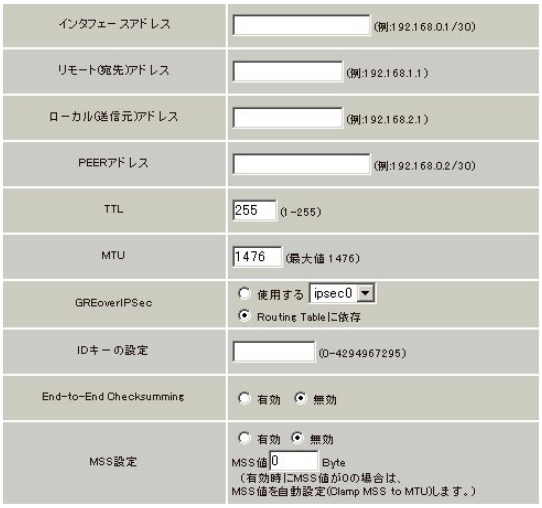
第 27 章

GRE 機能

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。また IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

設定画面「GRE 設定」→ GRE インタフェース設定をクリックして設定します。



○インタフェースアドレス
GRE トンネルを生成するインタフェースの仮想アドレスを設定します。任意で指定します。

○リモート(宛先)アドレス
GRE トンネルのエンドポイントの IP アドレス(対向側装置の WAN 側 IP アドレス)を設定します。

○ローカル(送信元)アドレス
本装置の WAN 側 IP アドレスを設定します。

○ PEER アドレス
GRE トンネルを生成する対向側装置のインタフェースの仮想アドレスを設定します。「インタフェースアドレス」と同じネットワークに属するアドレスを指定してください。

○ TTL
GRE パケットの TTL 値を設定します。

○ MTU
MTU 値を設定します。最大値は 1476byte です。

○ GREoverIPsec
IPsec を使用して GRE トンネルを暗号化する場合に「使用する」を選択して IPsec インタフェース名を選択します。またこの場合には別途、IPsec の設定が必要です。
「Routing Table に依存」は GRE トンネルを暗号化して使わないときに選択してください。

○ ID キーの設定
GRE パケットの識別用の ID を設定します。

○ End-to-End Checksumming
チェックサム機能の有効 / 無効を選択します。
この機能を有効にすると、
checksum field (2byte) + offset (2byte)
の計 4byte が GRE パケットに追加されます。

○ MSS 設定
GRE トンネルに対して、clamp to MSS 機能を有効にしたり、MSS 値の設定が可能です。

入力後は「追加 / 変更」ボタンをクリックします。直ちに設定が反映され、GRE が実行されます。

「削除」をクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

「現在の状態」では GRE の動作状況が表示されます。

GRE 設定をおこなうと、設定内容が一覧表示されます。

設定の編集は「Interface 名」をクリックしてください。また GRE トンネルのリンク状態は「Link State」に表示されます。「UP」が GRE トンネルがリンクアップしている状態です。

第 28 章

ゲートウェイ認証機能

ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。
この機能を使うことで、外部へアクセスできるユーザーを管理できるようになります。

◆基本設定

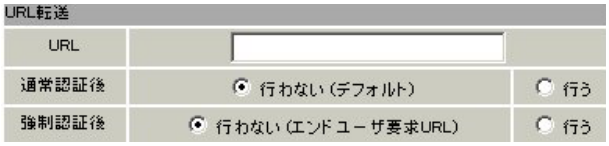
[基本設定]

○本機能
ゲートウェイ認証機能を使う場合は「使用する」を選択します。

○認証
当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。
認証を行わないときは「しない」を選択します。このときは、外部へのアクセスをリダイレクトするだけの動作となります。

○ 80/tcp 監視
認証を受けていない IP アドレスからの TCP ポート 80 番のコネクションを監視し、**このコネクションがあったときに、強制的にゲートウェイ認証をおこないます。**
初期設定は監視を「行わない」設定となります。

[URL 転送]



○ URL
転送先の URL を設定します。

○通常認証後
「はい」を選択すると、ゲートウェイ認証後に「URL」で指定したサイトに転送させることができます。初期設定では URL 転送を行いません。

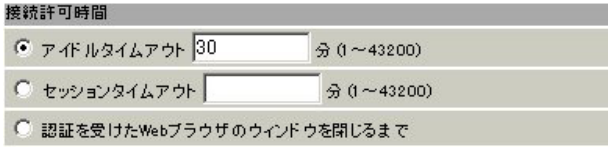
○強制認証後
「はい」を選択すると、強制認証後に「URL」で指定したサイトに転送させることができます。初期設定では URL 転送を行いません。この機能を使う場合は「80/tcp 監視」を有効にしてください。

[認証方法]

○認証方法
「ローカル」XR-410 でアカウントを管理 / 認証します。
「RADIUS サーバ」外部の RADIUS サーバでアカウントを管理 / 認証します。

ゲートウェイ認証機能の設定

[接続許可時間]



○接続許可時間
認証したあとの、ユーザーの接続形態を選択できます。

「アイドルタイムアウト」
認証で許可された通信が無通信状態となってから切断するまでの時間を設定します。

「セッションタイムアウト」
認証で許可された通信を強制的に切断するまでの時間を設定します。認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。

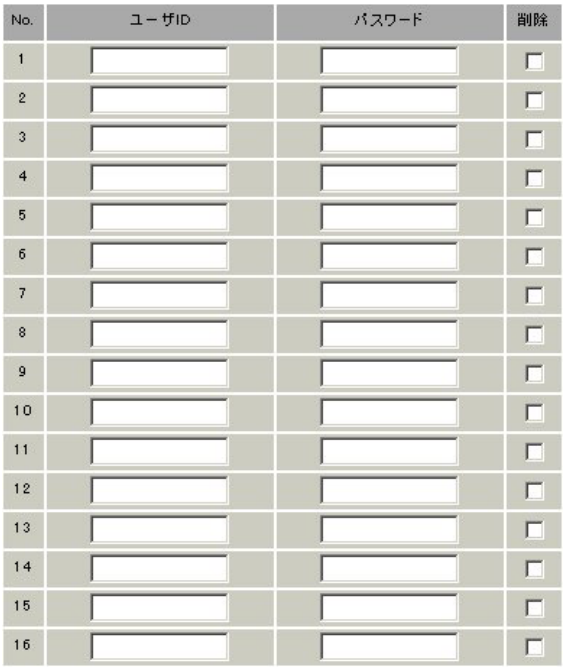
「認証を受けた Web ブラウザのウィンドウを閉じるまで 」
認証を受けた後にブラウザに表示された画面を閉じたときに、通信を切断します。通信可能な状態を保つには、認証後の画面を開いたままにしなければなりません。web ブラウジングをする場合は、別のブラウザを開く必要があります。

上記設定にしたがって通信が切断した場合は、各ユーザーは再度ゲートウェイ認証を実行する必要があります。

最後に「設定変更」をクリックしてください。

ゲートウェイ認証機能を「使用する」にした場合はただちに機能が有効となりますので、ユーザー設定等から設定をおこなってください。

◆ユーザー設定



○ユーザー ID・パスワード
ユーザーアカウントを登録します。
ユーザー ID・パスワードには半角英数字が使用できます。空白やコロン(:)は含めることができません。
「削除」をチェックすると、その設定が削除対象となります。

最後に「設定 / 削除の実行」をクリックしてください。

ゲートウェイ認証機能の設定

◆RADIUS 設定

「基本設定」において、認証方法を「RADIUS サーバ」に選択した場合にのみ設定します。

○プライマリ / セカンダリサーバ設定
RADIUS サーバの IP アドレス、ポート番号、secret を設定します。プライマリ項目の設定は必須です。セカンダリ項目の設定はなくてもかまいません。

○サーバ共通設定
RADIUS サーバへ問い合わせをする際に送信する NAS の情報を設定します。RADUIS サーバが、どの NAS かを識別するために使います。どちらかの設定が必須です。

”NAS-IP-Address”は IP アドレスです。通常は XR-410 の IP アドレスを設定します。

”NAS-Identifier”は任意の文字列を設定します。半角英数字が使用できます。

○アイドルタイムアウト
○セッションタイムアウト

RADIUS サーバからの認証応答に該当のアトリビュートがあればその値を使います。該当のアトリビュートがなければ「基本設定」で設定した値を使用します。それぞれ、基本設定で選択されているものが有効となります。

Idle-Timeout：アイドルタイムアウト
Ascend-Maximum-Time：セッションタイムアウト
Ascend-Idle-Limit：アイドルタイムアウト

※アトリビュートとは、RADIUS で設定されるパラメータのことを指します。

最後に「設定変更」をクリックしてください。

ゲートウェイ認証機能の設定

◆フィルタ設定

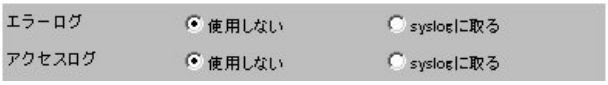
ゲートウェイ認証機能を有効にすると外部との通信は認証が必要となりますが、フィルタ設定によって認証を必要とせずに通信可能にできます。特定のポートだけはつねに通信できるようにしたいといった場合に設定します。

設定画面「フィルタ設定」をクリックします。”**「フィルタ設定」のゲートウェイ認証設定フィルタ設定画面 にて設定して下さい。**”というメッセージが表示されたらリンクをクリックしてフィルタ設定画面に移ります。

ここで設定した IP アドレスやポートについては、ゲートウェイ認証機能によらず、通信可能になります(設定方法については「第 25 章 パケットフィルタリング機能」をご参照下さい)。

◆ログ設定

ゲートウェイ認証機能のログを本装置のシステムログに出力できます。



ログを取得するかどうかを選択します。

・エラーログ ： ゲートウェイ認証時のログインエラーを出力します。
・アクセスログ ： ゲートウェイ認証時のアクセスログを出力します。

<エラーログの表示例>

```
Apr  7 17:04:45 localhost httpd[21529]:
[error] [client 192.168.0.1] user abc: au-
thentication failure for "/": password mis-
match
```

<アクセスログの表示例>

```
Apr  7 17:04:49 localhost authgw: 192.168.0.1
- abc [07/Apr/2003:17:04:49 +0900] "GET /
HTTP/1.1" 200 353
```

ゲートウェイ認証下のアクセス方法

◆ホストからのアクセス方法

①ホストから本装置にアクセスします。以下の形式でアドレスを指定してアクセスします。

http://<本装置の IP アドレス>/login.cgi

②認証画面がポップアップしますので、通知されているユーザー ID とパスワードを入力します。

③認証に成功すると以下のメッセージが表示され、本装置を経由して外部にアクセスできるようになります。

<認証成功時の表示例>

```
You can connect to the External Network
(abc@192.168.0.1).

Date: Mon Apr 7 10:06:51 2003
```

◆設定画面へのアクセスについて

ゲートウェイ認証機能を使用していて認証をおこなっていなくても、本装置の設定画面にはアクセスすることができます。アクセス方法は、通常と同じです。

◆ RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、XR-410 は RADIUS サーバに対して認証要求のみを送信します。

RADIUS サーバへの要求はタイムアウトが 5 秒、リトライが最大 3 回です。プライマリサーバから応答がない場合は、セカンダリサーバに要求を送信します。

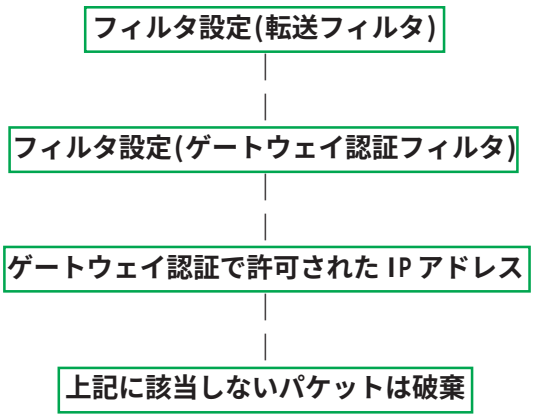
◆認証について

認証方法が「ローカル」の場合、HTTP Basic 認証を使って認証されます。
「RADIUS サーバ」の場合は、PAP で認証要求を送信します。

ゲートウェイ認証の制御方法について

ゲートウェイ認証機能はパケットフィルタの一種で、認証で許可されたユーザー(ホスト)の IP アドレスを送信元 / あて先に持つ転送パケットのみを通過させます。制御は、転送フィルタ設定の最後でおこなわれます。

フィルタリング制御の順番は以下の通りです。



ゲートウェイ認証機能を使わない場合は、通常の「転送フィルタ」のみ有効となります。

「転送フィルタ」に設定をしてしまうと、ゲートウェイ認証よりも優先してそのフィルタが参照されてしまい、ゲートウェイ認証が有効に機能しなくなる恐れがあります。

ゲートウェイ認証機能を使用する場合は、「転送フィルタ」には何も設定せずに運用してください。

第 29 章

ネットワークテスト

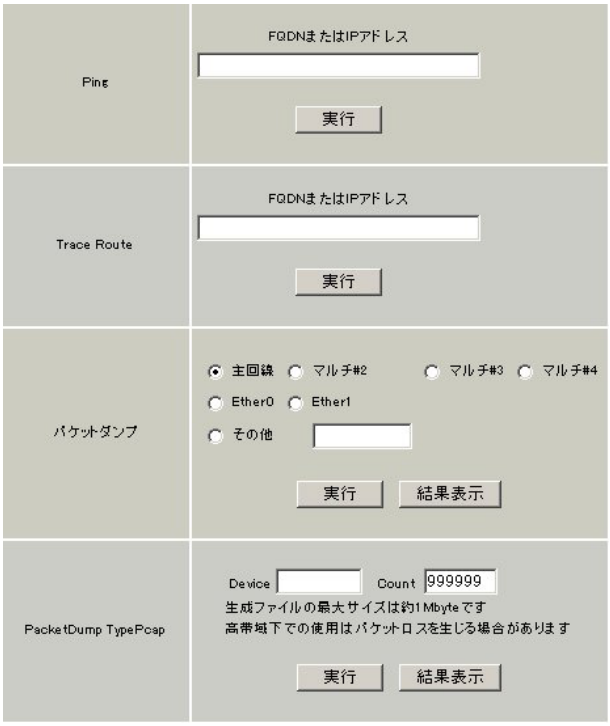
ネットワークテスト

XR-410 の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。以下の 3 つのテストができます。

- **ping テスト**
- **traceroute テスト**
- **パケットダンプの取得**

実行方法

Web 設定画面「ネットワークテスト」をクリックして、以下の画面でテストを実行します。



○ping テスト

指定した相手に XR-410 から Ping を発信します。FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms
64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms
64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms

--- 211.14.13.66 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 11.7/37.3/71.4 ms
```

○ traceroute テスト

指定した宛先までに経由するルータの情報を表示します。ping と同様に、FQDN もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=12.4 ms

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
traceroute to 211.14.13.66 (211.14.13.66), 30 hops max, 40 byte packets
 1  192.168.120.15 (192.168.120.15)  1.545 ms  2.253 ms  1.607 ms
 2  192.168.100.50 (192.168.100.50)  2.210 ms  4.955 ms  2.309 ms
 3  172.17.254.1 (172.17.254.1)  8.777 ms  21.189 ms  13.946 ms
 4  210.135.192.108 (210.135.192.108)  9.205 ms  8.953 ms  9.310 ms
 5  210.135.208.34 (210.135.208.34)  35.538 ms  19.923 ms  14.744 ms
 6  210.135.208.10 (210.135.208.10)  41.641 ms  40.476 ms  63.293 ms
 7  210.171.224.115 (210.171.224.115)  43.948 ms  27.255 ms  36.767 ms
 8  211.14.3.233 (211.14.3.233)  36.861 ms  33.890 ms  37.679 ms
 9  211.14.3.148 (211.14.3.148)  36.865 ms  47.151 ms  18.491 ms
10  211.14.3.105 (211.14.3.105)  53.573 ms  13.889 ms  50.057 ms
11  211.14.2.193 (211.14.2.193)  33.777 ms  11.380 ms  17.282 ms
12  * * *
13  211.14.12.249 (211.14.12.249)  19.692 ms !X *  15.213 ms !X
```

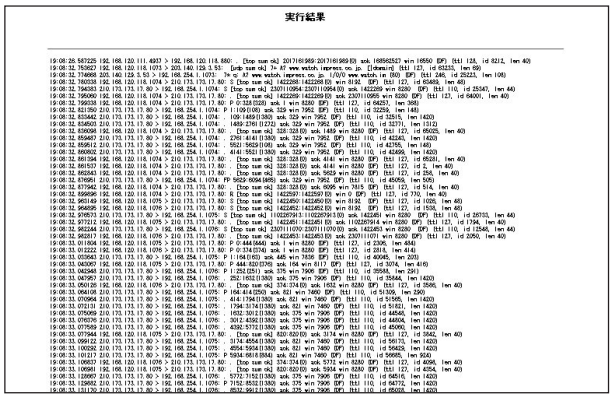
ping・traceroute テストで応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。その場合はまず、IP アドレスを直接指定してご確認下さい。

ネットワークテスト

○パケットダンプ

パケットのダンプを取得できます。
ダンプを取得したいインターフェースを選択して「実行」をクリックします。その他を選択し、直接インタフェース名を指定することもできます。その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例



「結果表示」をクリックするたびに、表示結果が更新されます。
パケットダンプの表示は、最大で 100 パケット分までです。100 パケット分を超えると、古いものから順に表示されなくなります。

○ PacketDump TypePcap

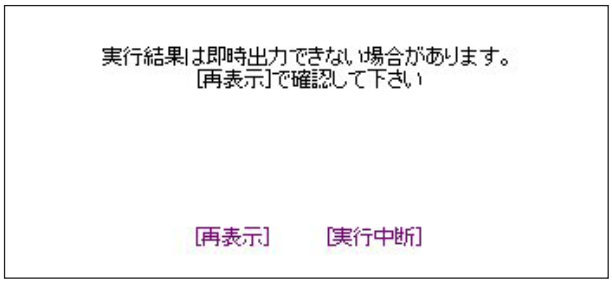
拡張版パケットダンプ取得機能です。
指定したインタフェースで、指定した数のパケットダンプを取得できます。

「device」：パケットダンプを実行する、本装置のインタフェース名を設定します。インタフェース名は「情報表示」画面で確認できます。

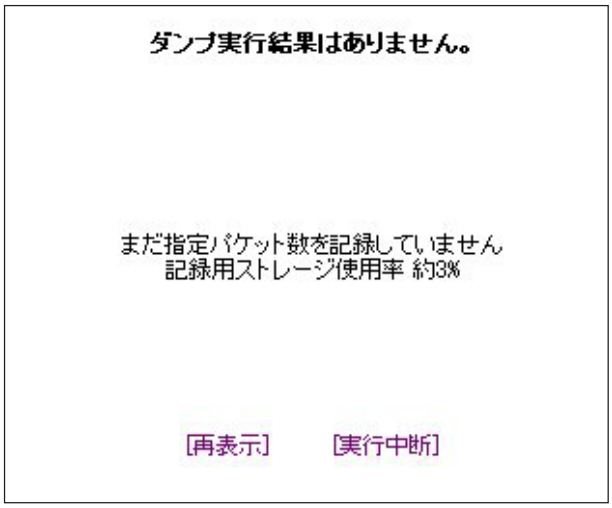
「Count」：パケットダンプの取得数を指定します。1 ～ 99999 の間で指定します。

上記項目を入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示



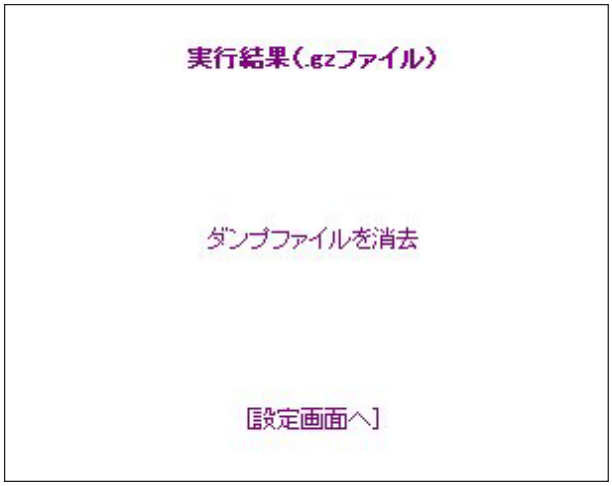
パケットダンプ結果を表示できないときの画面



パケットダンプ実行中に「再表示」ボタンをクリックすると、上記のような画面が表示されます。

ネットワークテスト

パケットダンプが実行終了したときの画面



「Count」で指定した数のパケットダンプを取得したとき、「実行中断」ボタンをクリックしたとき、またはパケットダンプ取得終了後に「結果表示」をクリックしたとき、上記の画面が表示されます。

「実行結果(.gz ファイル)」リンクから、パケットダンプ結果を圧縮したファイルをローカルホストに保存してください。

ローカルホスト上で解凍してできたファイルは、Ethereal で閲覧することができます。

「ダンプファイルを消去」をクリックすると、本装置に記録されているダンプファイルを消去します。

[PacketDump TypePcap の注意点]

・取得したパケットダンプ結果は、libcap 形式で gzip 圧縮して保存されます。

・取得できるデータサイズは、gzip 圧縮された状態で最大約 1MB です。

・本装置上にはパケットダンプ結果を 1 つだけ記録しておけます。パケットダンプ結果を消去せずに PacketDump TypePcap を再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。

[PacketDump TypePcap の注意点]

本装置のインタフェース名については、下記の表をご参照下さい。

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ehter2ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ppp6	アクセスサーバ(シリアル接続)
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
gre<n>	gre(<n>は設定番号)

第 30 章

各種システム設定

各種システム設定

「システム設定」ページでは、XR-410の運用に関する制御をおこないます。下記の項目に関して設定・制御が可能です。

- **時計の設定**
- **ログの表示 / 削除**
- **パスワード設定**
- **ファームウェアアップデート**
- **設定の保存・復帰**
- **設定のリセット**
- **本体の再起動**
- **セッションライフタイムの設定**
- **設定画面の設定**

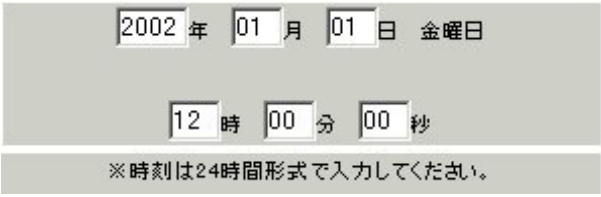
実行方法

Web設定画面「システム設定」をクリックします。各項目のページへは、設定画面上部のリンクをクリックして移動します。

◆時計の設定

XR-410内蔵時計の設定をおこないます。

「時計の設定」をクリックして設定画面を開きます。



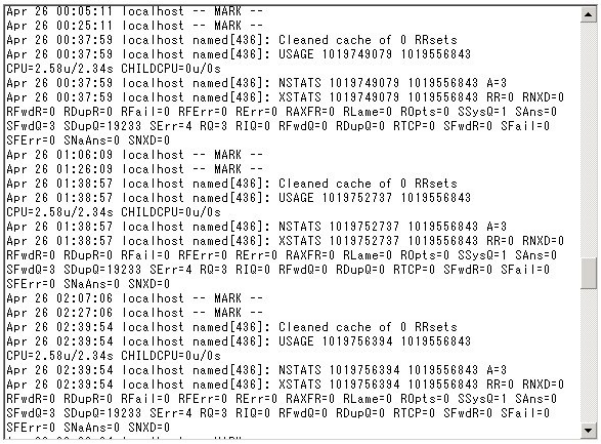
○24時間単位で時刻を設定してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。設定はすぐに反映されます。

各種システム設定

◆ログの表示

「ログの表示」をクリックして表示画面を開きます。



○XR-410 のログが全てここで表示されます。

○「表示の更新」ボタンをクリックすると表示が更新されます。

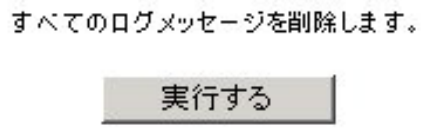
「不正アクセス検出機能」を使用している場合は、そのログも併せてここで表示されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

◆ログの削除

ログ情報は最大 2MB までのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

「ログの削除」をクリックして画面を開きます。



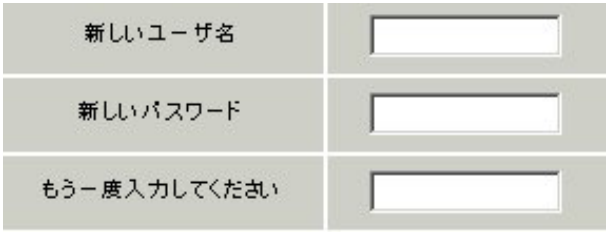
○「削除実行」ボタンをクリックすると、保存されているログが**全て削除**されます。

各種システム設定

◆パスワードの設定

XR-410の設定画面にログインする際のユーザー名、パスワードを変更します。ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

「パスワードの設定」をクリックして設定画面を開きます。



○新しいユーザー名とパスワードを設定します。半角英数字で 1 から 8 文字まで設定可能です。大文字・小文字も判別しますのでご注意下さい。

入力が終わりましたら「設定」ボタンをクリックして設定完了です。次回のログインからは、新しく設定したユーザー名とパスワードを使います。

◆ファームウェアのアップデート

XR-410 は、ブラウザ上からファームウェアのアップデートをおこないます。

1 「ファームウェアのアップデート」をクリックして画面を開きます。

2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

3 その後、ファームウェアを本装置に転送します(転送が終わるまではしばらく時間がかかります)。転送完了後に、以下のようなアップデートの確認画面が表示されますので、バージョン等が正しければ「実行する」をクリックしてください。

(次のページに続きます)

各種システム設定

上記画面が表示されたままで 3 分間経過すると、以下の画面が表示され、アップデートが実行されません。

アップロード完了から3分以上経過したため
ファームウェアは破棄されました

4 アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。

ファームウエアのアップデートを実行します。
作業には数分かかりますので電源を切らずにお待ち下さい。
作業が終了しますと自動的に再起動します。

アップデート中は、本体の LED が ”8” を表示します。この間は、アクセスをおこなわずにそのままお待ちください。

ファームウェアの書き換え後に本装置が自動的に再起動されて、アップデートの完了です。

◆設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

実行方法

「設定の保存・復帰」をクリックして画面を開きます。

- - 注意 - -

「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置の RSA の秘密鍵を含む設定情報等がネットワーク上に平文で流れます。
設定の保存・復帰は、ローカル環境もしくは VPN 環境等、セキュリティが確保された環境下で行う事をお勧めします。

上記のような注メッセージが表示されてから、「設定の保存・復帰」のリンクをクリックします。

[設定の保存]
設定を保存するときは、テキストのエンコード形式と保存形式を選択して「設定ファイルの作成」をクリックします。

現在の設定を保存することができます。	
コードの指定	○ EUC(LF) ◉ SJIS(CR+LF) ○ SJIS(CR)
形式の指定	○ 全設定(gzip) ◉ 初期値との差分(text)

クリックすると以下のメッセージが表示されます。

設定をバックアップしました。
バックアップファイルのダウンロード

ブラウザのリンクを保存する等で保存して下さい。

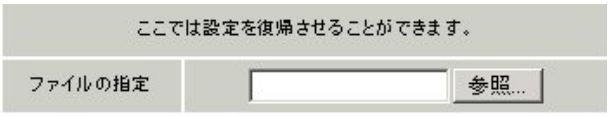
「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。

(次のページに続きます)

各種システム設定

「全設定」を選択すると、本装置のすべての設定をgzip形式で圧縮して保存します。
「初期値との差分」を選択すると、初期値と異なる設定のみを抽出して、テキスト形式で保存します。このテキストファイルの内容を直接書き換えて設定を変更することもできます。

[設定の復帰]
上記項目から「参照」をクリックして、保存しておいた設定ファイルを選択します。全設定の保存ファイルはgzip圧縮形式のまま、復帰させることができます。



その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

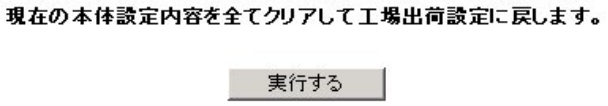
――注意――

「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のＲＳＡの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。設定の保存・復帰は、ローカル環境もしくはＶＰＮ環境等、セキュリティが確保された環境下で行う事をおすすめします。

◆設定のリセット

XR-410の設定を全てリセットし、工場出荷時の設定に戻します。

「設定のリセット」をクリックして画面を開きます。



「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

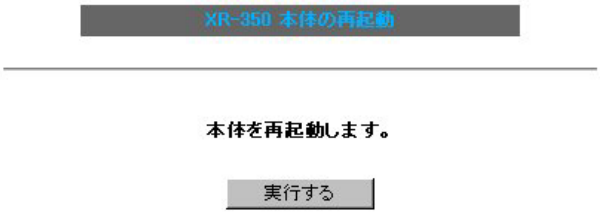
設定のリセットにより全ての設定が失われますので、念のために「設定のバックアップ」を実行しておくようにしてください。

各種システム設定

◆本体再起動

XR-410 を再起動します。設定内容は変更されません。

「再起動」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、リセットが実行されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

◆セッションライフタイムの設定

NAT/IP マスカレードのセッションライフタイムを設定します。

「セッションライフタイムの設定」をクリックして画面を開きます。

○ UDP

UDP セッションのライフタイムを設定します。単位は秒です。0 ～ 8640000 の間で設定します。初期設定は 30 秒です。

○ UDP stream

UDP stream セッションのライフタイムを設定します。単位は秒です。0 ～ 8640000 の間で設定します。初期設定は 180 秒です。

○ TCP

TCP セッションのライフタイムを設定します。単位は秒です。0 ～ 8640000 の間で設定します。初期設定は 432000 秒です。

「設定の保存」ボタンをクリックすると、設定が保存されます。設定内容はすぐに反映されます。

各種システム設定

◆設定画面の設定

WEB設定画面へのアクセスログについての設定をします。

実行方法

「設定画面の設定」をクリックして画面を開きます。

設定画面の

○アクセスログ
○(アクセス時の)エラーログ

を取得するかどうかを指定して、「設定の保存」をクリックします。

アクセスログ・エラーログは、「syslog」サービスの設定にしたがって出力されます。

第 31 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- **ファームウェアバージョン情報**
  現在のファームウェアバージョンを確認できます。

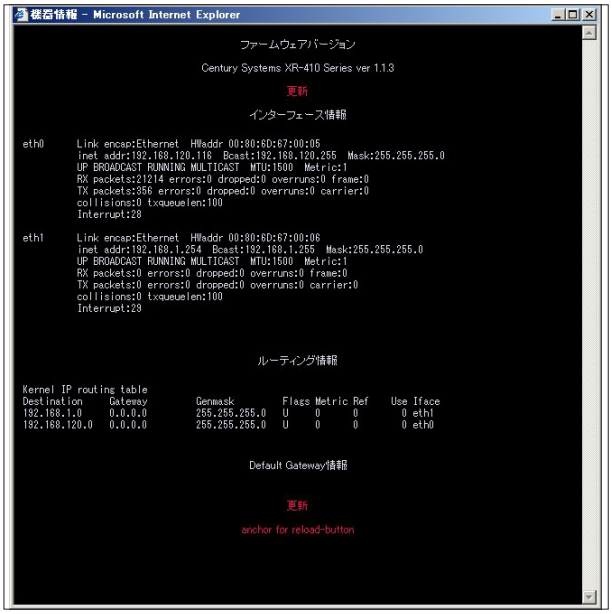
- **インターフェース情報**
  各インターフェースの IP アドレスや MAC アドレスなどです。
  PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。

- **ルーティング情報**
  デフォルトルート、ダイナミックルートを含めて現在保持しているすべてのルーティング情報です。

- **DHCP クライアント情報**
  DHCP クライアントとして設定しているインタフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

Web 設定画面「情報表示」をクリックすると、新しいウィンドウが開いて本体情報表示されます。



画面中の「更新」をクリックすると、表示内容が更新されます。

第 32 章

運用管理設定

一時的に工場出荷設定に戻す方法

XR-410 の背面にある「INIT ボタン」を使用して、XR-410 の設定を**一時的に工場出荷設定に戻す**ことができます。

INIT ボタンを押したまま電源切断→電源投入し、電源投入後も 5 秒ほど INIT ボタンを押しつづけると、本装置は工場出荷時の設定で再起動します。

ただしこのとき、工場出荷時の設定での再起動前の設定は別の領域に残っています。

この操作後にもう一度再起動すると、それまでの設定が復帰します。工場出荷時の設定で戻したあとに設定を変更していれば、変更した設定が反映された上で復帰します。

設定を完全にリセットする場合は、「システム設定」→「設定のリセット」でリセットを実行してください。

携帯電話による制御

XR-410 にグローバルアドレスが割り当てられていて、インターネットに接続している状態ならば、i モードおよび EZ ウェブに対応した携帯電話から以下のような操作が可能です。

- **ルータとしてのサービスを停止する**
- **ルータとしてのサービスを再開する**
- **本装置を再起動する**

この機能を利用する際は、パケットフィルタリング設定によって WAN 側からの設定変更を許す設定になっていることが必要になります。WAN 側から本装置の設定変更を許すフィルタ設定については「パケットフィルタ設定」ページをご覧下さい。

実際に操作画面にアクセスするためには、i モード端末から次の URL をしてしてください。

<i モード端末からアクセスする場合 >

http:// 装置の IP アドレス :880/i/

<EZ ウェブ端末からアクセスする場合 >

http:// 装置の IP アドレス :880/ez/index.hdml

アクセスすると認証画面が表示されますので、ユーザー名とパスワードを入力してください。

「i フィルタ起動」を実行すると、ルーターとしてのサービスが停止します。

この状態では、WAN から LAN へのアクセスはできません。WAN 側からは XR-410 自身の設定画面もしくは i モード画面にしかアクセスできなくなります。

また LAN 側からインターネット側へアクセスしても、アクセス先からの応答を受け取ることができなくなります。

「i フィルタ停止」を実行すると、以前の設定状態に戻り、ルーター機能が再開されます。

i モードからアクセスするには、パケットフィルタの「入力フィルタ設定」で、インターネット側から XR-410 の設定画面にログインできるように設定しておく必要があります。

IP アドレス自動割り当ての契約でインターネットに接続されている場合、XR-410 に割り当てられたグローバルアドレスが変わってしまう場合があります。もしアドレスが変わってしまったときは i モードからの制御ができなくなってしまうことが考えられますので(アドレスが分からなくなるため)、運用には十分ご注意下さい。

⇒ PPPoE で接続している場合に限り、「アドレス変更お知らせメール」機能を使って現在の IP アドレスを任意のアドレスにメール通知することができます。

携帯電話による操作方法

1 携帯電話端末から XR-410 の WAN 側に割り当てられたグローバルアドレスを指定してアクセスします。

2 ユーザー名とパスワードを入力して「OK」を選択します。

3 操作メニューが表示されます。

操作したい項目を選択して実行してください。

4 「フィルタ状態」を選択すると以下のような画面が表示されて、現在の状態を確認できます。

付録 A

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0

DHCPサーバ機能	有効
DHCPクライアント機能	無効
デフォルトゲートウェイ	設定なし
IPマスカレード機能	Ether0ポート以外で有効
NAT機能	設定なし
パケットフィルタ機能	ステートフルパケットインスペクション機能 (Ehter0ポート以外) NetBIOSの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定) 外部からのUPnPパケットを遮断する設定 (入力・転送フィルタ設定)
DNSリレー機能	有効
DNSキャッシュ機能	無効
スタティックルート設定	設定なし
ダイナミックルーティング	無効
IPsec機能	設定なし
GRE機能	無効
UPnP機能	無効
ログ機能	有効
DoS検出機能	無効
QoS(帯域制御)機能	無効
仮想インタフェース機能	設定なし
アクセスサーバ機能	無効
リモートアクセス機能	無効
SNMPエージェント機能	無効

設定画面ログインID	admin
設定画面ログインパスワード	admin

付録 B

製品仕様

◆ハードウェア仕様

製品名	FutureNet XR-410/TX2	FutureNet XR-410/TX2DES
CPU	400MHz	
暗号化処理	ソフトウェア	ハードウェア
OS	Linux Kernel 2.4.18	
通信インタフェース	Ether0 100/10 × 1ポート (LAN側) IEEE802.3u(100Base-TX)/IEEE802.3(10Base-T) コネクタ RJ-45(Auto MDI/MDIX) Ether1 100/10 × 1ポート (WAN側) IEEE802.3u(100Base-TX)/IEEE802.3(10Base-T) コネクタ RJ-45(Auto MDI/MDIX) RS-232 RS-232ポート(PPP接続用) × 1 9,600～230.4Kbps コネクタ RJ-45 RJ45⇔Dsub9ピン 変換コネクタ付属	
本体LED	ステータス (7セグメントLED)	
本体設定方法	Webブラウザ、設定ファイル 工場出荷値設定用のリセットボタン Webブラウザからのファームウェア更新機能	
環境条件	温度 0℃～＋40℃、湿度 25%～ 85% (結露なきこと)	
電波障害防止	VCCI クラスA 準拠	
JATE認定	D03-0229JP	
電源	DC5V 1A(最大)	
外形寸法	81mm(W)×117mm(D)×32.5mm(H)	
重量	約350g	
付属品	リリースノート、製品マニュアル PDF形式(CD-ROMに収録) RJ-45/D-sub9ピン変換アダプタ (ストレート仕様) UTPケーブル(ストレート)、AC電源ケーブル、保証書	
保証	購入日から１年間 センドバックによる対応	

◆ソフトウェア仕様

対応する接続形態	FTTH、ADSL、CATV、ローカルルータ PPPoE Unnumbered接続に対応
主な対応プロトコル	IP(IPV4)、IPsec(IPv4)、TCP、UDP、ICMP、ARP PPPoE、SMTP、HTTP、SNMP、GRE
IPルーティング方式	RIP、RIPv2、スタティック、デフォルトルート、OSPF
トンネリング機能	GRE64対地までサポート
DHCP機能	サーバ、クライアント、リレー（有効／無効）
NAT方式	1対1アドレス変換、IPマスカレード機能
静的NAT変換	バーチャルサーバ機能(最大128 IP、256エントリ) 送信元NAT機
ホスト名	CATV接続設定において設定可能
マルチPPPoEセッション	同時に最大4セッション
VPN機能（IPsec）	1対64拠点(最大)の構成、aggressiveモード対応 3DES/DES/AESでの暗号化処理
セキュリティ機能	パケットフィルタ、ステートフルパケットインスペクション DoS検出、パケット記録
QoS機能	帯域制御
パケットフィルタ機能	入力、転送、出力ごとに256ずつ設定可能 インタフェース、IN/OUT、制御方法、 IPアドレス プロトコル、ポートによる設定が可能
MACアドレスの変更	インタフェースをDHCPクライアントとした場合に 設定可能
高速化・チューニング	DNSキャッシュ機能、Proxy ARP、MTU設定
ログ機能	ブラウザ上での表示、メールでの送信機能 DoSログの取得 、自動トリミング機能
運用管理機能	i-mode,EZwebからの遠隔制御、電子メールによる ログ送信機能、設定ファイルによる一括設定 SNMPエージェント機能
リモートアクセス	リモートアクセス機能、アクセスサーバ機能
設定	WWWブラウザ上からおこなう
設定のバックアップ リストア	ブラウザ上から可能
バージョンアップ	ブラウザ上から可能
シリアルポート	インターネット接続機能、インターネットVPN機能、 アクセスサーバ機能 ※　PPPoEのバックアップ回線としても使用可能
その他	ゲートウェイ認証機能、パケットダンプ、ルータping発行

付録 C

サポートについて

付録 C

サポートについて

◆本製品に関してのサポートは、ユーザー登録をされたお客様に限らせていただきます。必ずユーザー登録していただきますよう、お願いいたします。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡下さい。

・サポートデスク
　電話 0422-37-8926
　受付時間　10:00～12:00 13:00～16:30　(土日祝祭日、及び弊社の定める休日を除きます)
・FAX　0422-55-3373
・e-mail　support@centurysys.co.jp
・ホームページ　http://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡下さい。事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンとＭＡＣアドレス
　(バージョンの確認方法は「第 31 章 情報表示」をご覧下さい)
・ネットワークの構成(図)
　どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせ下さい。
・不具合の内容または、不具合の再現手順
　何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせ下さい。
・エラーメッセージ
　エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
・XR-410 の設定内容、およびコンピューターの IP 設定
・**可能であれば、「設定のバックアップファイル」をお送りください。**

◆サポート情報
弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品の FAQ も掲載しておりますので、是非ご覧下さい。
XR-410 製品サポートページ
http://www.centurysys.co.jp/product/xr410/index_s.html

◆製品の保証について
本製品の保証期間は、お買い上げ日より 1 年間です。保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承下さい。保証規定については、同梱の保証書をご覧ください。

XR-410/TX2シリーズ ユーザーズガイド v1.4.1対応版
2004年5月版
発行 センチュリー・システムズ株式会社
2002-2004 CENTURYSYSTEMS,INC. All rights reserved.